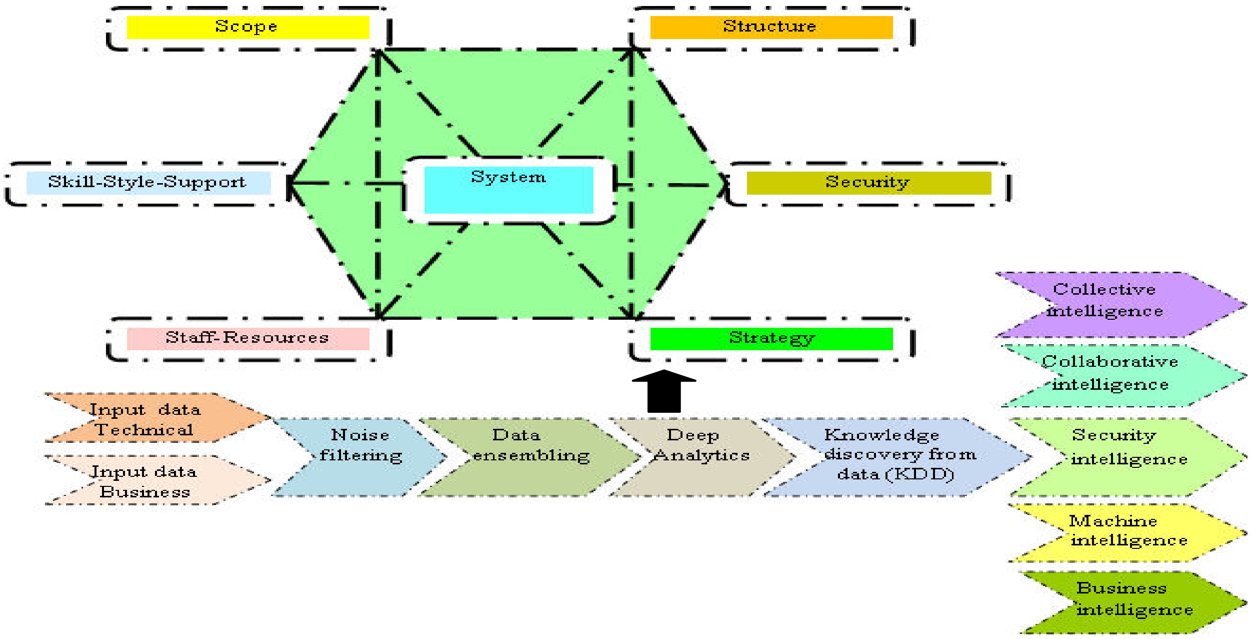
Deep Analytics:

Technologies for Humanity, AI & Security

1st Edition, 2021

By

Sumit Chakraborty
Suryashis Chakraborty
Kusumita Chakraborty



Natural disaster security : Artificial rainfall, Bushfire

Food & home security: smart agriculture, nanohousing

Education security : Learning policy, methodologies

Health security : cancer, biomedical technology, epidemic

Energy & utilities security: Solar power

Logistics Security: Electrical vehicles, DAS, RTFD

Financial security: Fault attacks, Sybil attack

Social security: social networking, digital governance, HRS

Digital technologies security : E-Governance

Preface

Deep analytics does not only mean statistics or data mining or big data analytics, it is a complex multi-dimensional analysis through '7-S' model based on rational, logical and analytical reasoning from different perspectives such as scope, system, structure, security, strategy staff-resources and skill-style-support. This book presents an analytical model through a consistent and systematic approach and highlights its utility and application for reasoning the complexity of a set of emerging technology innovations today: (a) Technology for humanity, (b) Deep analytics - '7-S' model, (c) Solar computing and self-healing mechanism, (d) Adaptive security for SCADA & Industrial Control System, (e) Secure Multi-party Quantum Computing, (f) Secure adaptive filter in adversarial environment, (g) Solar power electronics & Nanotechnology, (h) Electrical and hybrid vehicles : smart batteries, (i) RailTech security: Driver advice system & real-time fault diagnistics, (j) Cancer prediction and prevention: deep learning, (k) Biomedical technology for cancer care, (l) Natural disaster : epidemic and pandemic outbreak control, (m) Artificial rainfall, laser and cloud physics, (n) Real-time moving target search for astronomical hazards, (o) smart agriculture and nanhousing technology for smart cities and smart villages and (p) Emerging digital technologes for social, financial and education security. All the characters, sessions, plot and storyline of the technologies for humanity summit mentioned in this book are imaginative. Kusumita Chakraborty has contributed on education and social security and Suryashis Chakraborty has contributed on social and financial security.

The reality is that every stakeholder is impacted by the challenges and opportunities of innovation ecosystems today. The concept of technology for humanity and deep analytics is still relatively new; it has now emerged as a powerful tool for business analytics and a real world theme in the modern global economy. The target audience of this book includes academic and research community, corporate leaders, policy makers, administrators and governments, entrepreneurs, investors, engineers, producers and directors interested in production of documentary films, news and TV serials. We are excited to share the ideas of deep analytics with you. We hope that you will find them really value adding and useful and will share with your communities. It is a rational and interesting option to teach deep analytics in various academic programmes of various Business Management programmes (e.g. Technology Management, Human Resources Management, Information Technology, Information Systems, Management Information Systems (MIS), Strategic Management and Analytics for BBA, MBA, PGDM, PGDBM) and also Electrical and Electronics Engineering (e.g. B.Tech, M.Tech, B.E.E., M.E., Ph.D.). It is also interesting to produce TV serials, webseries and moviesand organize global summit on technologies for humanities based on the plot of this book. This e-book is the electronic version of 1st edition; Price: ($250 per copy). This book contains information obtained from authentic sources; sincere efforts have been made to publish reliable data and information. Thanks and regards.

Sumit Chakraborty, Fellow (IIM Cacutta), BEE (Jadavpur University), India.
Suryashis Chakraborty, BBA.
Kusumita Chakraborty, BA (Honours, Education), MA, Ph.D., CU, India
Business Analytics Research Lab, India. 1.1.2021

Content

SESSION 1: DEEP ANALYTICS - TECHNOLOGIES for HUMANITY and GLOBAL SECURITY

Event **: Technology for humanity and global security summit**
Venue**: Deep analytics hall, Technology park : Sanada**
Time Schedule **: 9 a..m. – 1 p.m. , 15.8.2020**
Agents **: Representatives of various global organizations (nations, childcare, peace, health, bank, economic forum), Technology management experts from science and technology forums, scientists, representatives and ministers from the departments of science and technologies of developed, developing and underdeveloped countries, CEOs of global corporations, business development consultants, representatives from NGOs.**
Key focus areas **: Deep analytics, 7-S model, Technologies for humanity, Global security, Sustainable development goals, Economic growth, Poverty, Jobs, Environmental protection, Business model innovation, Global welfare.**
Keynote speakers**: Prof. Nil Bajjio, Prof. Michel Johnson, Prof. Kalyan Som, Prof. David Milla, Dr. Rojer Moore, Dr, M. Schilling, Dr. S.Chakraborty.**

1. DEEP ANALYTICS

It is a sunny, windy morning. Seven hundred participants from all over the world have come to the technology park, Sanada to attend Technology for humanity and global security summit'2020. The President of Sanada has inaugurated the summit. It is an open forum; there are ten interactive brainstorming sessions; the participants are raising a set of debtable and intelligent questions on poverty, sustainable development goals, global security policy, business model innovation, economic growth and entrepreneurship. Dr. S.Chakraborty is presenting the basic overview of deep analytics. He is outlining the concept and mechanism of deep analytics to evaluate technology management in terms of seven 'S' elements (scope, system, structure, security, strategy, staff-resources and skill-style-support). He is also defining the significance of various parameters in the context of technology management such as technology security, technology classification, technology association, technology clustering, technology prediction or forecasting, innovation, adoption, diffusion, infusion and dominant design. The other objective of this session is to analyze the emerging concept of technology for humanity and select a set of emerging technologies for the sustainability of human civilization.

Deep analytics is an intelligent, complex, hybrid, multi-phased and multi-dimensional data analysis system [Figure 1.1]. The basic steps of computation are data sourcing, data filtering / preprocessing, data ensembling, data analysis and knowledge discovery from data. The authorized data analysts select an optimal set of input variables, features and dimensions (e.g. scope, system, structure, security, strategy, staff-resources, skill-style-support) correctly being free from malicious attacks (e.g. false data injection, shilling); input data is sourced through authenticated channels accordingly. The sourced data is filtered, preprocessed (e.g. bagging, boosting, cross validation) and ensembled. It is rational to adopt an optimal mix of quantitative (e.g. regression, prediction, sequence, association,

classification and clustering algorithms) and qualitative (e.g. case based reasoning, perception, process mapping, SWOT, CSF and value chain analysis) methods for multi-dimensional analysis. The analysts define intelligent training and testing strategies in terms of selection of correct soft computing tools, network architecture – no. of layers and nodes; training algorithm, learning rate, no. of training rounds, cross validation and stopping criteria. The hidden knowledge is discovered from data in terms of collective, collaborative, machine, security and business intelligence. The analysts audit fairness and correctness of computation and also reliability, consistency, rationality, transparency and accountability of the analytics.

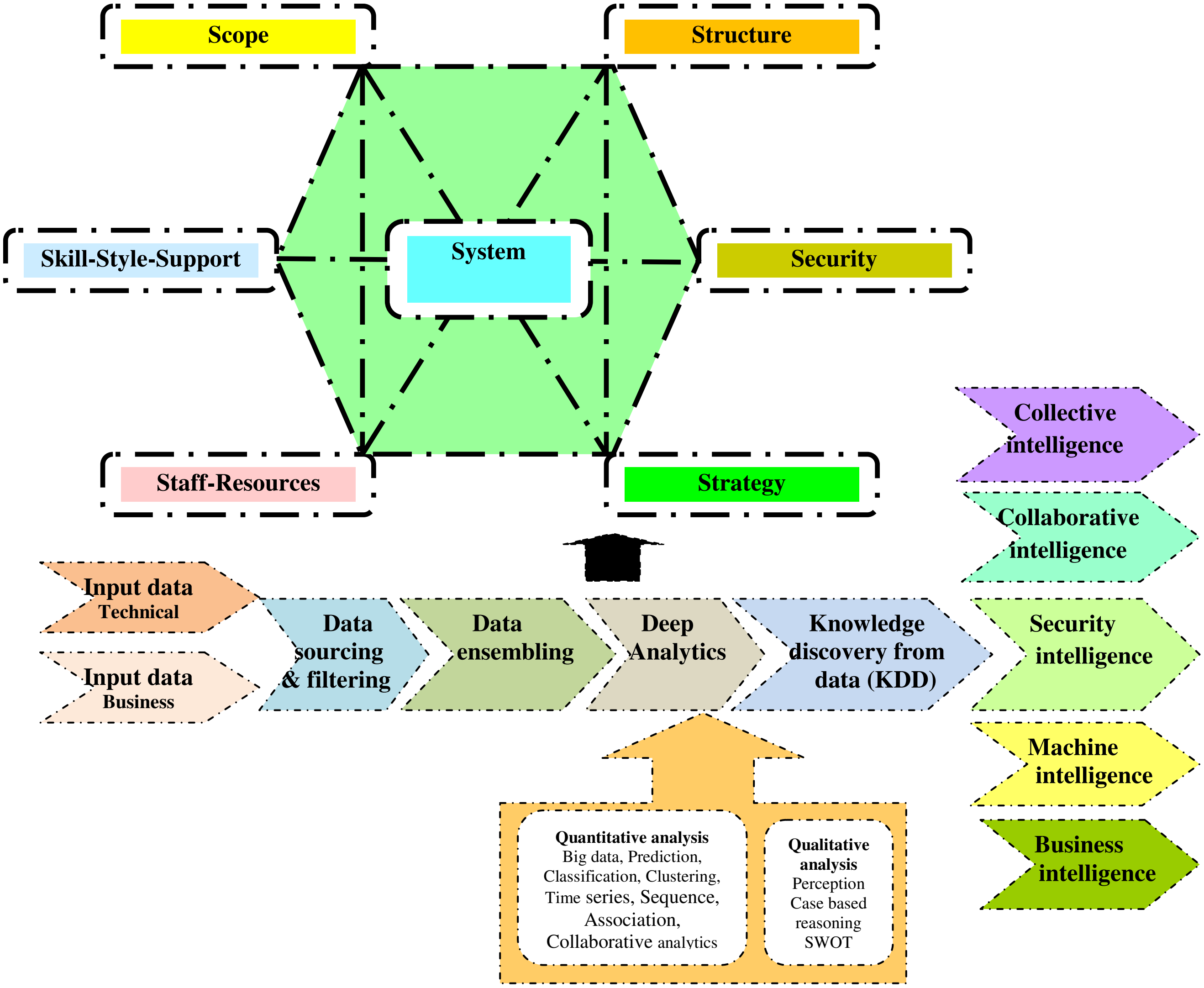


Figure 1.1 : Deep Analytics

Deep analysis can process precisely targeted, complex and fast queries on large (e.g. petabytes and exabytes) data sets of real-time and near real-time systems. For example, deep learning is an advanced machine learning technique where artificial

neural networks (e.g. CNN) can learn effectively from large amount of data like human brain learn from experience by performing a task repeatedly and gradually improves the outcome of learning. Deep analytics follows a systematic, streamlined and structured process that can extract, organize and analyze large amounts of data in a form being acceptable, useful and beneficial for an entity (e.g. individual human agent, organization or BI information system). It is basically a specific type of distributed computing across a number of server or nodes to speed up the analysis process. Generally, shallow analytics use the concept of means, standard deviation, variance, probability, proportions, pie charts, bar charts and tabs to analyze small data set. Deep analytics analyze large data sets based on the concepts of data visualization, descriptive and prescriptive statistics, predictive modeling, machine learning, multilevel modeling, data reduction, multivariate analysis, regression analysis, logistic regression analysis, text analysis and data wrangling. Deep analytics is often coupled with business intelligence applications which perform query based search on large data, analyze, extract information from data sets hosted on a complex and distributed architecture and convert that information into specialized data visualization outcome such as reports, charts and graphs. In this summit, deep analytics has been applied for technology management system (TMS).

Technological innovations are practical implementation of creative novel ideas into new products or services or processes. Innovations may be initiated in many forms from various sources such as firms, academic institutions, research laboratories, government and private enterprises and individual agents. There are different types of innovations from the perspectives of scope, strength, weakness, opportunities, threats and demands from the producers, service providers, users, service consumers and regulators.

Innovation funnel is a critical issue in technology management; innovation process is often perceived like a funnel with many potential ideas passing through the wide end of a funnel but very few become successful, profitable, economically and technically feasible products or services through the development process. Deep analytics is an intelligent method and consulting tool that is essential for effective management of top technological innovations today. It is basically an integrated framework which is a perfect combination or fit of seven dimensions. Many technological innovation projects fail due to the inability of the project managers to recognize the importance of the fit and their tendency to concentrate only on a few of these factors and ignore the others. These seven factors must be integrated, coordinated and synchronized for the diffusion of top technological innovations globally.

Deep Analytics Mechanism [DAM]

***Agents*: Single or a group of data analysts;**

***System* : Technology Management System /* Technology for humanity*/**

***Moves*:**

- **Adopt a hybrid approach : quantitative ⊕ qualitative;**
- **Optional choices :**
    - **Collaborative analytics /* agents : multiple data analysts*/**

- **Big data**
- **Predictive modelling**

***Objectives*: Evaluate an emerging technology for innovation, adoption and diffusion;**
***Constraints*: Availability of authenticated and correct data, time, effort, cost;**
***Input*: Technical data (D_t), Business data (D_b); /* Entity : An emerging technology for humanity*/**
***Procedure*:**

- **Source data (D_t, D_b);**
- **Filter data;**
- **Ensemble data;**
- **Analyze data → select choice**
  - ***Choice 1*: qualitative analysis (Perception, Case based reasoning, SWOT, TLC);**
  - ***Choice 2*: quantitative analysis (Prediction, Simulation);**
  - ***Choice 3* : Hybrid (quantitative ⊕ qualitative);**
- **Multi-dimensional analysis → KDD (S_1, S_2, S_3, S_4, S_5, S_6,S_7); /* S_1: Technology scope, S_2: System, S_3 : Structure, S_4: Technology security, S_5: Strategy, S_6: Staff-resources, S_7: Skill-style-support; KDD: Knowledge discovery from data */**

***Revelation principle*:**

- **Define information disclosure policy → preserve privacy of strategic data.**
- **Verify authentication, authorization and correct identification in data sourcing.**
- **Audit fairness, correctness, reliability, consistency and rationality of analytic computation.**

***Payment function* : Compare a set of technologies based on cost benefit analysis.**
***Output*: Technology intelligence (collective, collaborative, security, machine, business);**

Deep analytics is essential to understand the nature of a technological innovation and identify the gaps between as-is and to-be capabilities in a systematic and compelling way. It reasons seven dimensions under three major categories: (a) *Requirements engineering schema*: scope [S_1]; (b) *Technology schema* : system [S_2], structure [S_3], security [S_4] and (c) *Technology management schema* : strategy [S_5], staff-resources [S_6] and skill-style-support [S_7] [Figure 1.1]. This session analyzes each dimension briefly and reasons a set of cases of top technology innovations today in next sessions [2-10] applying the tool of deep analytics. The basic building blocks of our research methodology include critical reviews of existing works on technology management and case based reasoning. We have reviewed various works on technology management. We have collected the data of the cases from various technical papers and secondary sources. Session 10 concludes this summit.

2. SCOPE

Prof. Nil Bajjio is exploring the scope of deep analytics. Technological innovation is basically associated with new product development and new process innovation, act

and initiatives of launching new devices, methods or materials for commercial and practical applications. It is one of the most critical competitive drivers in many industries such as information and communication technologies, high technology manufacturing and life-science. Deep analytics explores miscellaneous issues of top technological innovations today such as dynamics of innovation, innovation strategy and implementation process; the impact of globalization of markets and advanced information and communication technologies, computer sided design, computer aided manufacturing, flexible manufacturing system, economic feasibility, economies of scale and short production run; technology life cycle, technology diffusion; social, environmental and economic effects, negative effects of technological changes; R&D fund allocation strategy; pace, advantages and disadvantages of innovation, critical success factors, causes of failure; cost optimization and differentiation. Technological innovations are essential to create new business models. But, many innovation projects fail to make profit due to various reasons such as scope creep or ill-defined scope analysis.

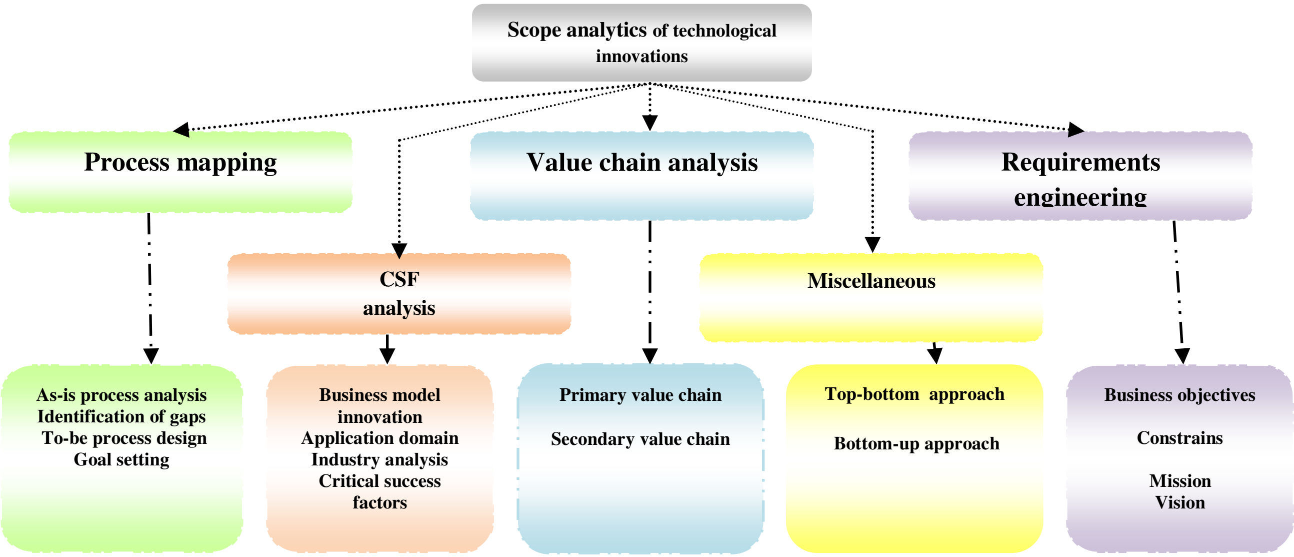


Figure 1.2 : Scope analytics

The first element of deep analytics is *scope*: How to define the goal of an emerging technology? The scope of a technology innovation project should be explored through various scientific and systematic methods such as sustainable goal setting, process mapping, critical success factors *(CSF) analysis*, *value chain analysis*, analysis of business objectives, constraints, requirements engineering, mission, vision and *top-down* and *bottom-up approaches* [Figure 1.2]. Process mapping analyzes a set of critical issues: what is as-is process? How to identify gaps of as-is process? How to innovate to-be process? What are the inputs, outputs, mechanism and constraint for each task associated with a business process? How to configure process flow diagram? The basic objective of CSF analysis is to identify a set of critical success factors through business model innovation, application domain and industry analysis.

The scope of a technology innovation project is explored based on CSFs. The basic objective of *value chain analysis* is to find out a set of critical parameters: what is value; it may be product differentiation, cost leadership or improved quality of services? How to define value in a technology innovation? What are the activities associated with primary and secondary value chain? Primary activities add value to a product and service directly such as manufacturing and supply chain management; secondary value chain activities (e.g. HR, Maintenance) support primary value chain activities. *Top bottom approach* analyzes business plans and goals of a firm, defines the basic needs of a system and explores the scope of technology innovation projects. On the other side, bottom up approach analyze as-is system, identifies gaps and explores the basic needs or scope of a project.

The scope of a technological innovation should be explored through *industry analysis* and also external environment and various stakeholders associated with the value chain. In this connection, *Porter's six force model* is useful to assess the bargaining power of the customers and suppliers, role of compliments, threats of new entrants and substitutes and competition. The internal environment should be accessed through SWOT analysis, identification of core competencies and rigidities, dynamic capabilities, potential strength and opportunities of sustainable competitive advantages. The scope should be also explored in terms of strategic intent, vision, mission and goals from different perspectives such as process innovation, organization learning, financial performance and customer satisfaction.

The scope of technological innovations may be analyzed from the perspectives of product or process innovation, radical or incremental, architectural or component and competence enhancing or destroying innovation. Product innovations occur in the outputs of a firm as new products or services. Process innovations try to improve the efficiency of business or manufacturing process such as increase of yield or decrease of rejection rate. Component or modular innovation changes one or more components of a product. Architectural innovation changes the overall design of a system or the way the components of a system interact with each other. Radical innovation is new and different from prior solutions. Incremental innovation makes a slight change of existing product or process.

We have explored a set of innovative concepts such as technology for humanity, cancer genomics, separating chromosomes, DNA computing, large scale cheap solar electricity and photovoltaics technology, solid state batteries, synthetic cells, next generation predictive, collaborative and pervasive analytics, big data analytics, adaptive security and dynamic data protection, secure adaptive filter, secure multi-party quantum computing, smart transformers, applied AI and machine learning, deep learning, assisted transportation, Internet of Things (IoT), cloud computing and cloud streaming, Internet of bodies, Blockchain and distributed ledger technology, homomorphic encryption, crash-proof code, social indexing, gestural interfaces, social credit algorithms, advanced smart material and devices, activity security protection, virtual reality, chatbots, automated voice spam prevention, serverless computing, edge computing, real-time ray tracing, digital twins, tablets and mobile devices in enterprise management, innovative mobile applications and interfaces for a multichannel future, human computer interface, context aware

computing and social media, enterprise app stores and marketplaces, in-memory computing, extreme low energy servers and strategic global sourcing.

The expert panel are defining technology for humanity and debating on its relevance today from the perspectives of sustainable development goals, global security policy and welfare, economic growth, poverty, new job opportunities, business model innovation, environmental pollution, skill development and talent management. They have selected a set of interesting and emerging technologies for the sustainability of human civilization. Some of these technologies are at emergence or birth phase of technology life-cycle: deep analytics, solar computing, adaptive security, secure adaptive filter and secure multi-party quantum computing. The other technologies are growing at moderate rate. Another objective of this session is to explore the concept of technology security, technology transition, technology classification, technology association, technology clustering, technology prediction and innovation, adoption and diffusion of technologies for humanity globally.

Scope Analytics

***Agents*: System analysts, business analysts, technology management consultants;**
***Objects / entities*: sustainable smart cities, smart villages, communities, smart world, smart universe;**
***Moves* : Critical success factors analysis, Process mapping, Value chain analysis, Requirements management;**
***Global security parameters*: define a set of sustainable development goals.**

- **Poverty control**
  - **Food security (zero hunger)**
  - **Home security (disaster proof nano-housing schema)**
  - **Garments and consumer goods security**
  - **Education security**
  - **Healthcare security (good health, well being, family planning, population control)**
  - **Financial security (banking, financial services, tax, insurance, retirement planning, stock and derivative trading, economic growth)**
  - **Energy security (clean and affordable renewable energy)**
  - **Utilities security (clean water and sanitaion, gas, computing, internet, telecom)**
  - **Communication security (internet, broadcast, satellite communication)**
  - **Logistics security (travel, hospitalities, surface, water, rail, water, EVs and hybrid vehicles)**
  - **Information, media and entertainment security**
- **Social security (HR security, decent work, religious and cultural security, gender equality, child security, women's empowerment, peace, justice, partnership, regulatory compliance, strong institutions)**
- **Natural disaster security (climate change, flood, drought, storm, cyclone, earthquake, volcano, snowfall, rainfall, fire, bushfire, global warming, heat wave, epidemic, astronomical hazards) (attack of wild animals, insects,**

paste); artificial disaster security (defense, war, act of terrorism, bioterrorism)

- ✪ Responsible consumption and production (Enterprise Resource Planning, Supply Chain Management)
- ✪ Industry, innovation and infrastructure (smart cities, smart villages)
- ✪ Life on land (environmental pollution, conservation of resources and forest, population control)
- ✪ Life below water (marine life, water pollution, global warming, oil leakage, nuclear explosion)

Technology for humanity involves integrated strategic planning, forecasting, design, optimization, operation and control of miscellaneous technological products, processes and services for the sustainability of human civilization and to understand the dynamics of technology innovation, hype, priority, capability, maturity, adoption, diffusion, infusion, transfer, life-cycle, dominant design, spillover effects, blind spots and also the value of emerging technologies for our society. How do we define 'Technology for humanity'? In our society, there is very little discussion about what is needed to fundamentally improve our collective quality of life through fundamental rethinking and radical redesign of systems and processes. How do we evolve our societies into something more productive, more rewarding and more in harmony with our natural environment against various threats of disaster? Emerging technologies can not only improve the world in which we live, they can alter who we are as human beings and can shape and improve our quality of life. The next big tech trend is technology for humanity. It is hard to visualize a roadmap from industry, government, academia & R&D communities of what future jobs and the economy might offer to people and what society might look like. By historic measures, future predictions are mostly incorrect. We need a better balance in our thoughts in terms of fairness, correctness and rationality. There is no reason why man and machine cannot work together, with humans at the controls. There is no reason why we cannot make decent investment returns and create meaningful job opportunities through business model innovation and new technologies build communities and protect the environment from pollution. Technology for humanity is definitely about putting the human society back into technology led globalization.

2020 is the year of coming out of the hype of old, traditional, dead and obsolete technologies. Realistically, it involves the critical role of human innovators in shaping a set of emerging technologies to improve the state of humanity. Technology is an enabler, the human society need to aggressively deploy it to address the critical issues of human society globally. These are basically sustainable development goals. Global goals are a universal call to action to end poverty, protect the planet from natural disasters and environmental pollution and ensure that our society enjoy peace and prosperity through business model innovation and creating new jobs opportunities using our human and technological superpowers and imagination. It is humanity and technology working together to solve various problems, assess and mitigate risks properly. The society have to allocate and share resources (e.g. man , machine, material, method and money) rationally and optimally by trading off risk and return intelligently. The society have to learn how to make acceptable risk adjusted returns eliminating hunger and poverty, creating employment diversity at

decent wages and cleaning up the planet. The society can no longer reward behaviors and outcomes that put humanity, communities and the planet in existential jeopardy. There is no point in arguing about a few % better return on capital when half of the world is underwater.

The expert panel are exploring the scope of technologies for humanity based on global security policy and a set of sustainable development goals. What is goal? There are different types of goals such as process goals (with control), performance goals and outcome goals (with least control). Can we define a rational global security policy? What should be the goals for a rational global security policy? How can we define sustainability: is it possible to meet the needs of the present society without compromising the ability of future generations to meet their own needs? What are Sustainable Development Goals (SDGs) or global goals for the sustainability of human civilization: can we protect our planet, the Earth, even this great universe by ensuring peace and prosperity and ending poverty?

Let us analyze the rationality, fairness and correctness of global security policy? What should be the vision of future world: universal respects for human rights and dignity, the rule of law and justice for equality and non-discrimination, end of hunger and improved nutrition through food security and sustainable agriculture, ensuring healthy life-style and promoting well-being for all at all ages, ensuring inclusive and equitable quality education, promotion of lifelong learning opportunities for all, gender equality and women empowerment. This goal setting demands the commitment, self-determination and trust among all nations to take necessary actions against climate change, unemployment, poverty and environmental pollution. It is crucial to maintain global security, peace, cooperation, collaboration and equality to solve economic, social, cultural and humanitarian problems. The basic objective is to define a set of universal goals that meet the urgent economic, political and environmental challenges facing our world.

Sustainable Development Goals (SDGs) are a collection of global goals to achieve a better and more sustainable future for all within a specific timeline: no poverty, zero hunger, good health and well-being, quality education, gender equality, clean water and sanitation, affordable and clean energy, decent work and economic growth, industry, innovation, and infrastructure, reducing inequality, smart cities, villages and communities, responsible consumption and production, climate action, life below water, life on land, peace, justice, strong institutions and partnerships for goals. The goals are broad based and interdependent. Is it possible to innovate a set of emerging technologies for humanity to achieve sustainable development goals and to track and visualize progress towards the goals through a set of performance indicators?

3. SYSTEM

Prof. Michel Johnson is analyzing the second element of deep analytics - system [Figure 1.3]. A system is a complex grouping of interrelated parts i.e. machines and agents; it can be decomposed into a set of interacting sub-systems. A system may have single or multiple objectives; it is designed to achieve overall objectives in the best possible way. It is possible to analyze a system from the perspectives of system

state, complexity, model, environment, system dynamics, cause effect analysis, feedback loop, physical and information flows and policy decisions. A system may be open or closed loop. A hard system clearly defines objectives, decision making procedures and quantitative measures of performance. It is hard to define the objectives and qualitative measures of performance and make decisions for a soft system. The state of a system at a specific time is a set of relevant properties of the system. The complexity of a system can be analyzed in terms of number of interacting elements, number of linear and nonlinear dynamic relationships among the elements, number of goals or objectives and number of ways the system interacts with its environment. A model is an abstraction of real system. A model is isolated from its environment through model boundaries. A model may be static or dynamic, linear or non-linear based on functional relationship among various variables in a model.

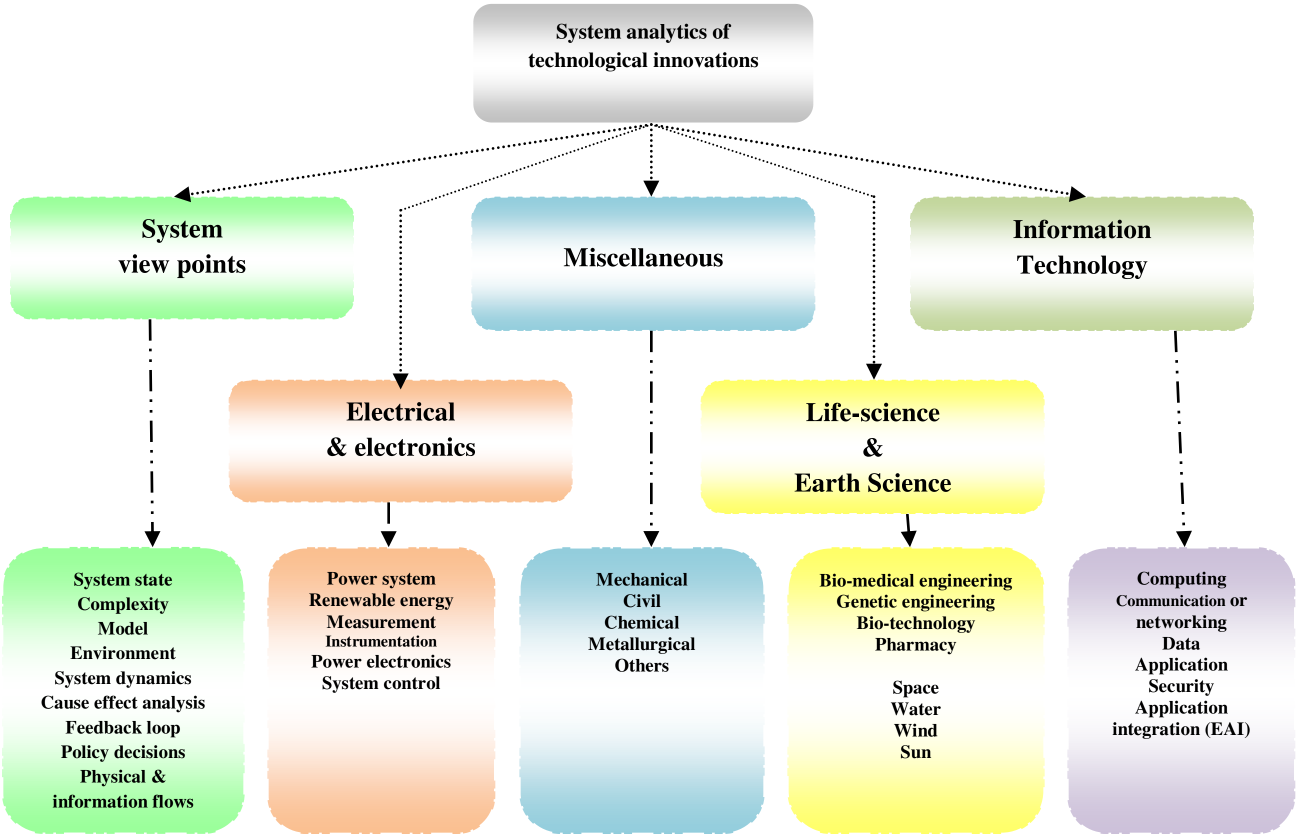


Figure 1.3 : System analytics

A complex system can be analyzed from the perspectives of different branches of engineering and technology such as information and communication technology, electrical and electronics, mechanical, civil, chemical, metallurgical, biotechnology, genetic engineering, pharmacy and others. IT system can be analyzed in terms of computing, communication or networking, data, application and security schema and also application integration (EAI). An electrical system may have various

subsystems such as power system, renewable energy, photonics, system control, power electronics, machines, measurement & instrumentation, illumination and high voltage engineering. A complex system may be associated with various domains of earth science such as space science, water, wind and solar power.
The basic objective of system analytics is to analyze complex, dynamic, non-linear and linear interactions in various types of systems and design new structures and policies to improve the behavior of a system. A system is associated with a problem oriented model; the basic building blocks of system dynamics are cause effects analysis, positive and negative feedback loops and physical and information flows. The basic functions of system analytics include defining a problem and model boundary, building model, testing and validation of a model, model analysis, evaluation of policy alternatives and recommendation of most viable R&D policy related to technological innovations.

System Analytics

Agents: **System analysts, business analysts, technology management consultants;**
Objects / entities: **sustainable smart cities, smart villages, communities, smart world, smart universe;**
Moves : **Requirements engineering, system design, coding, prototype testing, erection, installation, testing, commissioning**
Emerging technologies: **Innovate a set of emerging technologies based on global security parameters and sustainable development goals. /* Refer to scope analytics, section 1 */**

- **Poverty control**
  - **Food and beverage security (zero hunger):Automation in agricultural engineering and animal husbandries (dairy, poultry, epiculture, sericulture), biotechnology, genetic engineering (seeds), (chemical (organic fertilizer, paste controllers), electrical (solar water pump), civil, mechanical (solar power enabled tractors), food processing, digital technologies (warehouse management system, ERP, SCM, CPFR);**
  - **Home security : disaster proof nano-housing schema, roof-top solar panels, civil, mechanical, metallurgical, virtual reality;**
  - **Garments and consumer goods security : chemical (jacket, rain coats), textile, agriculture, process manufacturing, retail;**
  - **Education security : digital technology, innovation on education policy (TQM), education methodology, education technology, education materials;**
  - **Healthcare security (good health, well being, family planning, population control): Biomedical technology (laser, surgical robotics), life-science, pharmaceutical, pharmacy, biotechnology, digital technology, artificial intelligence (artificial immune system, soft computing and machine learning, deep learning, case based reasoning), precision medicine, genomics), technology related to R&D**

on biological science (biology, botany, zoology, human physiology, microscope), mechatronics;

- **Financial security (banking, financial services, tax, insurance, retirement planning, stock and derivative trading, economic growth) : Digital technology, information and communication technology, computers, electrical (solar power), electronics, civil, mechanical;**
- **Energy security (clean and affordable renewable energy) : solar microgrid, wind power, power plant technology, mechanical, civil, digital technology (AI enabled smart grid);**
- **Utilities security (clean water and sanitation, gas, computing, internet, telecom): Petrochemical, chemical, electrical (solar power enabled induction cooker), water purifier, wireless communication;**
- **Communication security: web technology, internet, broadcast communication, satellite communication;**
- **Logistics security (travel, hospitalities, surface, water, rail, water): Electrical and hybrid vehicles, Automobile technology, mechanical, electrical (electrical cycles and scooters, solar power enabled battery charging), metallurgy, chemical (carbon), water cycles, water scooters, drones, electronics (sensors, global positioning system), digital (Driver advice system);**
- **Information, media and entertainment security : digital technology (SOC, SOA), cloud computing, quantum computing, secure adaptive filter, solar computing, soft computing, AI, deep analytics, data science, business intelligence, electronics (smart TV, smart phones);**

- **Social security (HR security, decent work, religious and cultural security, gender equality, child security, women's empowerment, peace, justice, partnership, regulatory compliance, strong institutions): digital technology (E-Governance, Social networking, e-court, AI enabled legal system, case based reasoning);**
- **Natural disaster security (climate change, flood, drought, storm, cyclone, earthquake, volcano, snowfall, rainfall, fire, bushfire, global warming, epidemic, astronomical hazards) (attack of wild animals, insects, paste); artificial disaster security (war, act of terrorism, bioterrorism) : Earth science, artificial rainfall, cloud physics, artificial immune system, real-time moving target search for astronomical hazards, music system;**
- **Responsible consumption and production : digital technology (ERP, SCM);**
- **Industry, innovation and infrastructure (smart cities, smart villages): civil, mechanical, electrical, electronics, metallurgy;**
- **Life on land (environmental pollution, conservation of resources and forest, population control): environmental engineering, sensors, earth science;**
- **Life below water (marine life, water pollution, global warming, oil leakage, nuclear explosion): environmental engineering, sensors, earth science, marine technology;**

Let us explore requirements engineering of technologies for humanity for the people of our society and the planet, now and into the future. At its heart are the aforesaid sustainable development goals which are an urgent call for action by all developed and developing countries of the world through strategic alliance and global partnership. The fundamental building block of technologies for humanity is business model innovation - how is it possible to create new job opportunities against the threats of environmental pollution (e.g. air, water, soil, sound and light pollution)? Who are the customers and service consumers? Who are the service providers or the selling agents? What do the customers value? What should be the revenue and profit generation streams of an emerging technology? How to deliver value to the customers at appropriate cost? Following table 1.1 outlines a set of global security parameters and related emerging technologies for humanity. The next sessions (2-10) have shown the complexity analysis of these technologies in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support.

4. STRUCTURE

Prof. David Milla is analyzing the third element of deep analytics - structure i.e. the backbone of a system associated with a specific technological innovation [Figure 1.4]. What are the basic elements of the system architecture associated with a technology innovation? It has two critical viewpoints: system architecture and organization structure. The first one considers technological aspects of the system architecture in terms of topology, smart grid and various components of industrial control system such as SCADA, Expert system, DCS, PCS, SIS, BAS and EMS. The topology of a system should be analyzed in terms of nodes, connectivity, type of connections such as P2P or multipoint, layers, interfaces between layers and organization of layers.

For example, OSI model is a layered framework for the design of communication networks of information systems. It has seven layers from bottom to top : physical, data link, network, transport, session, presentation and application layers. A data communication system has five basic components such as message, sender, receiver, transmission medium and protocol. On the basis of nodes and links, the physical topology of a communication network can be classified into four categories such as mesh, ring, star and bus. The second viewpoint is organization structure – what type of structure is suitable for specific technological innovation; it may be functional, divisional, matrix or network structure. Is there any link between technology and organization structure? It depends on the characteristics of business model.

Another view of structure should be explored in terms of organization structure, size of a firm, economies of scale in R&D, access to complementary resources such as capital and market, governance mechanisms and organizational learning. There are various types of organization structure such as divisional and networked models. The efficiency and creativity of innovation model is closely associated with different types of structural dimensions such as formalization, standardization, centralization, decentralization and loosely coupled networks within and between

firms. Global firms should consider several critical factors such as knowledge, resources and technological diffusion to conduct R&D activities.

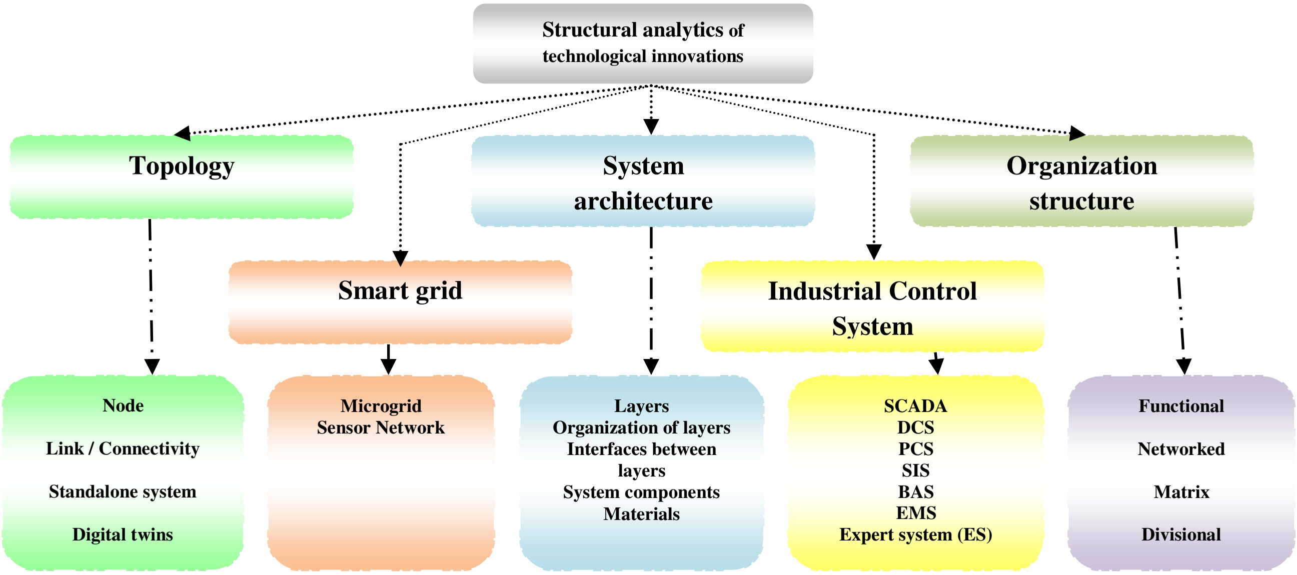


Figure 1.4: Structure analytics

How is it possible to represent the structure of a system associated with a technology innovation correctly and transparently? Digital twins may be an interesting solution; it integrates the concept of industrial IoT, AI, machine learning and software analytics to optimize the operation and maintenance of physical assets, systems and manufacturing processes. A digital twin is the digital replica of a living or non-living physical entity (e.g. physical asset, process, agent, place, system, device); it is expected to bridge and support data sharing between the physical and virtual entities. Digital twins can learn from multiple sources such as itself through sensors, historical time series data, experts and other nodes of the networking schema of the system and get updated continuously to represent real-time status, working conditions or positions.

The concept of digital twins are expected to be useful for manufacturing, energy (e.g. HVAC control systems), utilities, healthcare and automotive industries in terms of connectivity, digital traces and product life-cycle management. The concept can be used for 3D modeling to create digital companions of the physical objects i.e. an up-to-date and accurate copy of the properties and states of the objects (e.g. shape, position, gesture, status, motion) based on the data collected by the sensors attached to the system. It may be useful for the maintenance of power generation equipment such as turbines, jet engines and locomotives; monitoring, diagnostics and prognostics to optimize asset performance and utilization through root cause analysis and to overcome the challenges in system development, testing, verification and validation for automotive applications. The physical objects are virtualized and can be represented as digital twin models seamlessly and closely integrated in both physical and cyber spaces. Digital twins should represent the structure of a product innovation intelligently through various phases of the product life-cycle.

Another interesting technology for exploring innovative structure is V-commerce through virtual (VR), mixed (MR) and augmented reality (AR). A virtual entity may not exist physically but created by software in a digital environment. VR and AR are sophisticated, creative and powerful tools to show complex structures and offer a complete computerized digital experience by integrating AI, computer vision, graphics and automation in various applications such as manufacturing, retail, healthcare, entertainment, furniture and interior decoration.

Structure Analytics

***Agents*: System analysts, business analysts, technology management consultants;**

***Objects / entities*: sustainable smart cities, smart villages, communities, smart world, smart universe;**

***Moves*: Design and configure /* refer to scope and system analytics, sections 1 and 2 */**

- **Organization structure**
    - **Technology forums, innovation research laboratories, technical and management institutes, libraries / digital libraries;**
    - **National level : Government , E-governance model; academy-industry integration, research organizations, ;**
    - **International level : strategic alliance among global organizations alliance (nations, heath, child, peace), joint ventures, enterprise integration;**
    - **National, multinational and global organization;**
- **System architecture (topology, modules, nodes, connectivity, layers);**

***Emerging technologies* : Innovate a set of emerging technologies based on global security parameters and sustainable development goals. Construct a technology tree.**

***Level 1*: digital technology, information technology, computer science, earth science, environmental engineering, agriculture engineering, genetic engineering, electrical, electronics, telecommunication, sensor, renewable energy, power plant, instrumentation, biomedical, biotechnology, pharmacy, chemical, mechanical, nanotechnology, mechatronics, automobile, civil, construction, architecture, chemical, petroleum, oil and gas, metallurgy;**

***Level 2* : Identify technology classification and technology association in the technology tree.**

- **Information technology**
    - **Computing schema**
    - **Data schema: RDBMS, Datawarehousing, Data mining, Analytics, Data Visualization, Performance scorecard;**
    - **Networking schema**
    - **Application schema**
    - **Security schema**
- **Electrical technology - Power electronics, Electrical machines, Power system, Renewable energy, Measurements and instrumentation, High voltage engineering, Control system, Illumination;**

- **Electronics - Telecommunication, Biomedical electronics, Digital electronics, Optoelectronics;**
- **Mechanical - Materials science, Mechatronics, Robotics, Hydraulic Engineering, Heat Engines, power plant, Automobiles;**
- **Civil - Construction, Architecture;**
- **Chemical - Inorganic, Organic;**
- **Metallurgical**
- **Healthcare engineering - Pharmacy, Biotechnology, Life science, Biomedical engineering**

5. SECURITY

Prof. Kalyan Som is analyzing the fourth element of deep analytics - security [Figure 1.5]. What do you mean by technology-security? A system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real time to detect any anomalies, vulnerabilities or malicious traffic congestion and. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of a system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks.

Let us explain the objectives of adaptive security architecture in depth. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for the emerging technologies. The systems demand continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

How to verify the security intelligence of the system associated with an emerging technology? It is essential to verify security intelligence of a technological innovation collectively through rational threat analytics at five levels : L1, L2, L3, L4 and L5 (Figure 1.5). It is essential to assess risks associated with an emerging technology and mitigate the risks by adopting a set of countermeasures. The basic building blocks of the security element are an adversary model and an intelligent threat analytics. An adversary is a malicious agent who attacks a system or a protocol; the basic objectives are to cause disruption and malfunctioning of a secure system. The security element should be analyzed in terms of the assumptions, goals and capabilities of the adversary. It is also crucial to analyze the adversary model in

terms of environment, location, network, resources, access privileges, equipments, devices, actions, results, risks, reasons and motivations of attacks and probable targets (i.e. why the adversary attacks and to obtain what data).

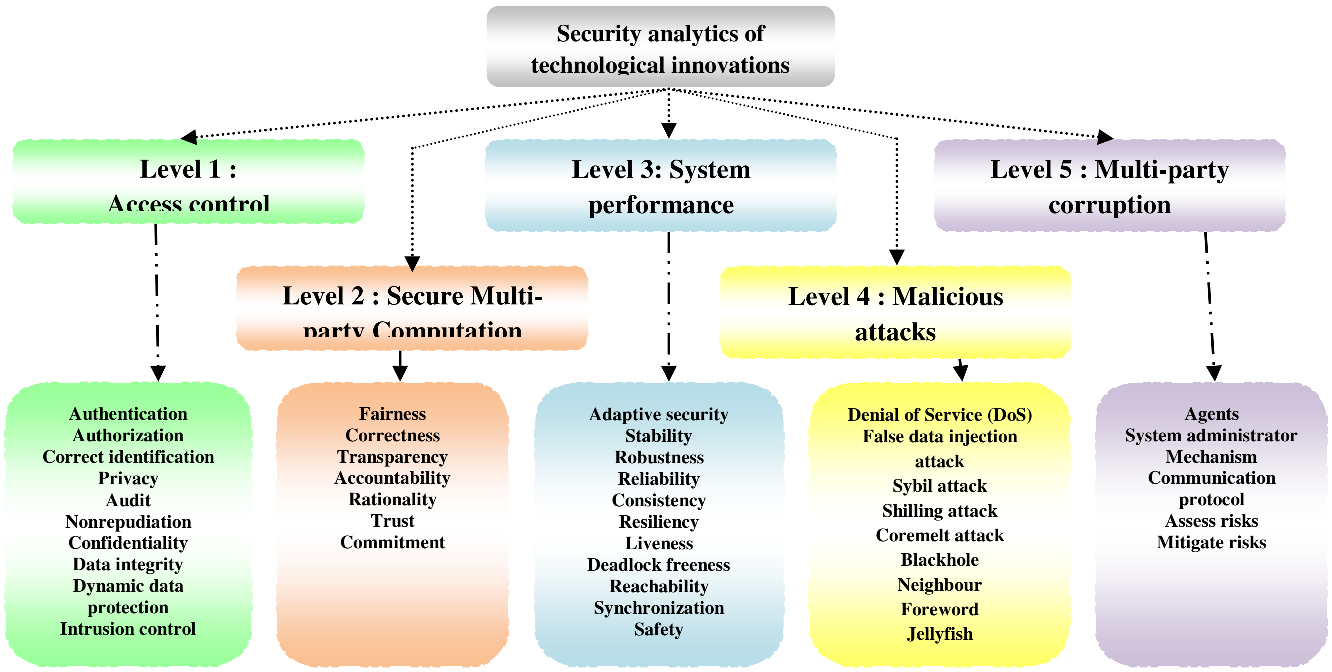


Figure 1.5 : Security analytics

Let us consider the security of an information system innovation. At level L1, it is required to verify the efficiency of access control in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, non-repudiation and data integrity. For any secure service, the system should ask the identity and authentication of one or more agents involved in a transaction. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries.

After the identification and authentication, the system should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication.

Privacy is the primary concern of the revelation principle of an information system; the issue of secure private communication can be addressed through the concept of cryptography, digital signature, signcryption and secure multiparty computation.

The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption methods. Data integrity ensures that data is protected from unauthorized modifications or false data injection attack. The system should provide public verifiability so that anyone can verify the integrity of the data. Redundancy of data is a critical issue which is resulted through replication across the writers.

Traditionally, cryptographic solutions are focused to ensure information security and privacy. But there are other different types of security concerns. At level L2, it is required to verify the efficiency of secure multiparty computation associated with a technological innovation in terms of fairness, robustness, correctness, transparency, accountability, trust and commitment. A protocol ensures correctness if the sending agent broadcasts correct data and each recipient receives the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with the commitment, honesty and rational reasoning on payment function, trust and quality of service. Fairness ensures that something will or will not occur infinitely often under certain conditions. The recipients expect fairness in private communication according to their demand plan, objectives and constraints. The sending agent expects fairness from the recipients in terms of true feedback and commitment on confidentiality of data. As per traditional definition of fairness of secure multi-party computation, either all parties learn the output or none. The system must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. In fact, accountability is also associated with collective intelligence. Transparency is associated with communication protocols, revelation principle and automated system verification procedures. For example, a mechanism should clearly state its goal to define a policy. There exist an inherent tension between transparency and privacy. A fully transparent system allows anyone to view any data without any provision of privacy. On the other side, a fully private system provides no transparency. Privacy can be achieved using cryptographic techniques at increased cost of computation and communication. Is it possible to trade-off privacy vs. transparency? Is it possible to provide public verifiability of its overall state without disclosing information about the state of each entity? Public Verifiability allows anyone to verify the correctness of the state of the system.

Next, it is required to verify the system performance at level L3 in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety. The performance of a system and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Safety is a critical requirement of any system whether it may be mechanical, electrical, electronics, information technology, civil, chemical, metallurgical or instrumentation engineering. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. Another important issue is robustness of

a system. The delivery of the output should be guaranteed and the adversary should not be able to threaten a denial of service attack against a protocol.

At level L4, it is required to assess the risks of various types of malicious attacks by adversaries on a system such as Denial of Service (DoS), false data injection attack, sybil attack, shilling attack, coremelt attack (or network traffic congestion), blackhole, neighbor, node deletion, rushing and jellyfish attacks. At level L5, it is required to assess the risks of various types of corruptions such as agents (e.g. sending agent, receiving agents), system administrator, communication protocol and payment function of a mechanism associated with a technological innovation.

For example, prevention and detection are traditional approaches to the security of a system. In today's world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security but should adopt cloud based solutions and open application programming interfaces also. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture.

Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjusts individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of the system and complexity of networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

Security Analytics

***Agents*: System analysts, business analysts, technology management consultants;**
***Objects / entities*: sustainable smart cities, smart villages, communities, smart world, smart universe;**
***Global security parameters*: define a set of sustainable development goals. /* Refer to scope and system analytics, sections 1 and 2 */**

***Verification algorithm* : audit *security intelligence* of emerging technology innovation.**

- ***access control*: verify authentication, authorization, correct identification, privacy, audit confidentiality, data integrity and non-repudiation;**
- ***computational intelligence*: verify rationality, fairness, correctness, transparency, accountability, trust and commitment;**
- ***system performance* of SOA: verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness, reachability, synchronization, safety;**
- ***malicious attacks*: verify the risk of Sybil, false data injection, shilling: push and pull, denial of service (DoS), coercion or rubber hose attack, fault injection attack, node replication wormhole, blackhole, neighbor, jellyfish, coremelt attack;**
- ***web security:* session hijack, phishing, hacking, cross site request forgery, cross site script, broken authentication, improper error handling;**
- ***multi-party corruption:* system analysts, business analysts, system administrators, innovators;**

call threat analytics and assess risks of emerging technologies:

- **what is corrupted or compromised (agents, computing schema, communication schema, data schema, application schema)? detect type of threat.**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights : how and why did it occur? do cause-effect analysis on performance, sensitivity, trends, exception and alerts.**
- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**

***Output*: security intelligence**

It is essential to verify security intelligence of emerging technologies for humanity collectively through rational threat analytics. The security intelligence is a multi-dimensional parameter which should be verified at multiple levels. Each emerging technology must be developed and audited by a group of authorized agents such as business analysts, system analysts and system administrators. The scope of BBIS should be correctly identified in terms of a set of corporate functions and performance metrics; relevant data should be sourced through authenticated raters. The system should preserve confidentiality and privacy of the raters and system administrators, nonrepudiation and integrity of data. For business performance measurement, the system should ask the identity and authentication of the raters. After correct identification and authentication, the system should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task. The raters and analysts should be assigned an explicit set of access rights according to role. Privacy is another important issue; the analysts and the raters can view only the information according to authorized access rights.

It is also crucial to verify the computational intelligence of BBIS in terms of fairness, correctness, rationality, transparency, accountability, trust and commitment. The raters are expected to provide fair and correct rating of each performance metric through proper justification, evidence, examples and case studies. The trust and commitment of the raters should be validated by the system administrator. The scorecard may be corrupted by dishonest raters, system administrators, business and system analysts, data visualization and data interpretation schema.

The web enabled scorecard must evaluate the corporate performance and the related financial impact in terms of reliability, consistency, resiliency, liveness and stability. The performance of the system is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that the system should never be in a state in which no progress is possible. The scorecard should be protected from various types of malicious attacks such as false data injection attack, fault attack, denial of service attack, Sybil attack, shilling attack (push and pull attack). The raters should not be able to inject false data to push or pull the performance of an entity incorrectly. The BBIS system is expected to be an interactive system through which the raters can justify the quality of reasoning and decision making capabilities.

The scorecard is expected to be a resilient system. The resiliency measures the ability to and the speed at which the web enabled system can return to normal performance level following a disruption in survey. The system administrator face a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the service oriented architecture? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in project vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do system monitoring.

Let us try to ask a set of basic questions to define security: what is poverty? what are the causes of poverty? what are the effects of poverty? How can we assess risks of poverty? How can we mitigate the risks of poverty? How can we create new jobs through business model innovation? How can we fight against environmental pollution? What should be rational public policy to ensure social security? Traditionally, poverty means not having enough money to satisfy the basic needs of life such as food, clothing, home, education, healthcare, energy and utilities. Many poor people may have jobs, but do not earn enough money to satisfy the aforesaid basic needs. The World Bank has defined poverty in absolute terms. The bank defines extreme poverty as living on less than US$1.90 per day and moderate poverty as less than $3.10 a day. It was as been estimated that in 2008, 1.4 billion people had consumption levels below US$1.25 a day and 2.7 billion lived on less than $2 a day. Rural poverty is often caused by poor infrastructure that hinders development, mobility and agricultural activities (e.g. access to agricultural inputs

and markets). Without roads, the rural poor people are cut off from technological development and emerging markets in urban zones. The causes of child poverty may be poor parents, adult poverty, government policies, lack of education, unemployment, social services, disabilities and discrimination.

Poverty is not just lack of money; it is not having the capability to realize one's full potential as a human agent. It is a multidimensional problem and each dimension requires a different solution. There is no one gun to shoot all the problems in a simple way: the problems of healthcare or food are different from those of education or energy. Monetary dole may work to reduce desperation to some extent. The poor people should have access to essential resources of living at optimum level. But, there are several other constraints. The rich and super rich people of urban zone are often involved in overconsumption of resources. There are threats of intrusion, infiltration and migration of refugees who may consume resources of a country or a state irrationally through various ways.

Let us consider an example. The refugees of country B are migrated to country I at mass scale. Those refugees try to capture the essential resources of life of the people of country I through strategic alliance and local colony development and try to capture job market aggressively. The local people of country I become the victims of poverty and get unemployed due to the economic stress caused by the intrusion and infiltration of the refugees from country B. The problem may be extended to the migration of people from a poor, underdeveloped and unfertile state to a developed state of a country. Therefore, irrational resource consumption by the rich and super rich classes and intrusion, migration and infiltration of the refugees may be critical causal factors of poverty. Existing works on poor economics and poverty should address these issues critically. What should be the strategy for the intruders or refugees? Country I should help country B for the economic and social development through collaborative planning, emerging technology transfer and effective rehabilitation programmes for the poor refugees. Border security force may not be able to control the intrusion correctly.

The innovation, adoption and diffusion of emerging technologies are expected to improve the growth rate of economy at macro level and profits and market shares of the firms at micro level. For developing countries, access to emerging technology should boost nation's economy by reducing the cost of production, saving of labour, automation, growth of new business models, intelligent communication system, optimal capacity utilization, allocation and distribution of various natural resources. It is hard to fight against climate change such as global warming Poverty increases health risks due to food insecurity; poor children may have lower birth weight and life expectancies. It is interesting to explore the scope of technology for humanity: how to create jobs through business model innovation and economic growth through industrial revolution. There are other various issues of human resource management such as minimum wage, pay equity, paid leave and paid sick days and rational work schedules. Social security is crucial for the poor people who are unable to satisfy the basic needs of life such as food, clothing, housing, education, healthcare, energy and utilities. The social development occurs if a society can apply technological advances and reflect the same to their social life. Economic development improves the standard of living and quality of life of a

nation from low to high income economy. Science, Technology, Engineering and Mathematics (STEM) is important to ensure social, financial and information security globally today.

Poverty reduction or alleviation is a set of economic and humanitarian measures to ensure social and financial security. Can we explore and innovate a set of emerging technological solutions to ensure physical, social, information and financial security globally such as sustainable energy through solar power, improved agricultural technology and farming methods (e.g. fertilizers, pesticides, high yield seeds, water sewage), access to clean drinking water, conservation of water, increased access to education through Internet, intelligent waste management, social empowerment through advancement of information and communication technologies, improved and safe transportation (e.g. carpool, walk, cycling, bike or taking public transit), mobile healthcare, mobile banking, natural disaster management and adoption of reduce-reuse-recycle for environmental protection (e.g. reusable bags. avoiding plastic, less printing, save water and energy)?

The topmost goal of global security policy is to regulate poverty control i.e. no poverty and end poverty in all its forms everywhere by 2030. Extreme poverty has been cut by more than 50% since 1990. Still, around 1 in 10 people live on less than the target figure of international $1.25 per day. A very low poverty threshold is justified by highlighting the need of those people who are worst off. Poverty is more than the lack of income or resources: people live in poverty if they lack basic services such as healthcare, security, and education and experience hunger, social discrimination, and exclusion from decision making processes. Multidimensional Poverty Index should be used to monitor poverty globally.

Emerging and innovative agriculture technologies should be applied to end hunger through food security, improved nutrition and sustainable agriculture. It is crucial to improve agricultural productivity and incomes of small-scale food producers through sustainable food production systems and improving land and soil quality. Agriculture is the single largest employer for 40% of the global population and largest source of income for poor rural households. Women make up about 43% of the agricultural labor force in developing countries and over 50% in Asia and Africa; but own only 20% of the land. It is possible to ensure food security through advanced agriculture and food processing technologies (e.g. maintaining genetic diversity of seeds, increasing access to land, preventing trade restriction and distortions in world agricultural markets to limit extreme food price volatility, eliminating waste through International Food Waste Coalition, and ending malnutrition and undernutrition of children).

Advanced effective life-science, healthcare, biomedical engineering and biotechnologies should be applied to ensure health security through universal health coverage, access to essential medicines and vaccines, to end the preventable death of newborns and children under 5 and to end epidemics (e.g. AIDS, tuberculosis, malaria, and water borne diseases) and prevention and treatment of substance abuse, deaths and injuries from traffic accidents and from hazardous chemicals and air, water and soil pollution and contamination. Global security policy should focus on good health and well-being for people for all at all ages by increasing life

expectancy and reducing common killers of child and maternal mortality. Another critical area is cancercare.

Emerging digital technologies (e.g. Internet, TV, Radio) should be used to provide inclusive and equitable quality education and promote lifelong learning opportunities for all. Major progress is expected in access to education, specifically at the primary school level, for both boys and girls. The number of out-of-school children has reduced from 112 million in 1997 to 60 million in 2014. Still, at least 22 million children in 43 countries miss out on pre-primary education; 103 million youth worldwide still lack basic literacy skills and more than 60 percent of those are women. Massive open online courses (MOOCs) are free open education offered through online platforms to a wider audience. Education for Sustainable Development (ESD) is defined as education that encourages changes in knowledge, skills, values and attitudes to enable a more sustainable and equitable society. It aims to empower and equip current and future generations to meet the needs using a balanced and integrated approach to the economic, social and environmental dimensions of sustainable development.

Emerging technologies should be used to ensure energy security in terms of affordable, reliable and sustainable clean energy for all by increasing the share of renewable energy (e.g. solar power, wind power) in the global energy mix, improving energy efficiency and enhancing international cooperation to facilitate more open access to clean energy technology and more investment in clean energy infrastructure. Another challenge is to ensure drinking water supply, availability and sustainable management of water and sanitation for all. 6 out of 10 people lack safely managed sanitation services and 3 out of 10 lack safely managed water services globally. Safe drinking water and hygienic toilets can protect people from diseases due to water pollution.

Manufacturing is a major source of employment in our society. It is crucial to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation in discrete, batch and continuous production technology, to improve manufacturing value added per capita in developing world and improve productivity and yield. Modern construction, mechanical, electrical and electronics engineering and nano-housing technologies must be applied to develop smart cities and villages and inclusive, safe, resilient, and sustainable human settlements. It is crucial to give access to safe and affordable housing in densely populated slum areas. ERP and SCM systems should be used to monitor responsible consumption and production of essential resources through various means such as eco-friendly production methods and reducing the amount of waste by recycling and reuse in developed and developing countries. We must take precautions and proper actions to combat against climate change, global warming and extreme weather conditions by regulating emissions and promoting developments in renewable energy such as solar and wind power.

Innovative biological technologies, rational and regulated business practice and advanced marine science should be used to protect life below water, to conserve and sustainably use the oceans, seas and marine resources for sustainable development, to mitigate adverse effects of increased ocean acidification, water pollution and

negative impact on marine biodiversity. Oceans cover 71% of the Earth's surface making the planet livable. Rainwater, drinking water and global climate are regulated by ocean temperatures and currents. Over 3 billion people depend on marine life for their livelihood. Oceans absorb 30% of CO_2 produced by humans. The oceans contain about 200,000 species. Oceans are the world's largest sources of protein. But, the marine world is facing various types of threats such as marine pollution at shocking levels (e.g. 15 tons of plastic are released into the oceans per minute), 26% increase in acidification, death of 30 percent of marine habitats, death of 1 million sea birds and 100000 marine mammals overexploitation of 30% of world's fish stocks, Marine biodiversity is currently at stake due to extinctions, invasions, hybridizations and reductions in species.

Intelligent technologies and Geographical Information Systems (GIS) should be applied to protect life on land and to preserve biodiversity of forest, desert, and mountain eco-systems as a percentage of total land mass. It is crucial to protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss. It is a hard challenge to regulate land loss due to flood and drought and protect endangered species. Emerging digital technologies i.e. information and communication technologies should be applied for peace, justice and strong institutions. It is crucial to promote peaceful and inclusive societies for sustainable development, provide access to justice for all, build effective, accountable and inclusive institutions at all levels and regulate violence, sex trafficking, forced labor, child abuse and various types of crime through real-time, online data tracking system, universal legal identity and birth registration, nationality right, civil rights and easy access to AI enabled justice and social services.

Emerging technologies should be applied to promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all. Long term economic growth and infrastructure investment should be prioritized properly. Sustainable tourism may create new jobs. It is also essential to strengthen domestic financial institutions through trade related technical assistance for least developed countries and increase aid for trade support for developing countries is considered essential to economic development. An interesting sustainable development goal is to reduce income inequality within and among countries for shared prosperity through adoption of mobile commerce and digital payment technologies in banking, retail and financial services. It is also crucial to ensure gender equality through women empowerment and employment; it is not only a fundamental human right, but a necessary foundation for a peaceful, prosperous and sustainable world. It is essential to regulate child marriage.

Emerging digital technologies should be also applied to strengthen the means of implementation and revitalize the global partnership for sustainable development. It is essential to share knowledge, expertise, technology and financial support for global cooperation and public-private partnerships using digital technologies. This requires promotion of multidisciplinary and transdisciplinary research across economic, socio-political, and environmental sectors. Commitments should be

transformed into effective actions requiring a correct perception of target populations and must address all vulnerable groups such as children, elderly folks, persons with disabilities, refugees, indigenous peoples, migrants, and internally displaced persons.

6. STRATEGY

Dr, M. Schilling is analyzing the fifth element of deep analytics - strategy [Figure 1.6]. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovations are closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of top innovations today. Diffusion is the movement of molecules from high density zone to low density zone of a solution. Can an emerging technology diffuse in the same way globally? What is the pressure acting on technology diffusion? Is the external pressure natural or artificial? Another analogy is osmosis where the molecules move from low density zone to high density zone through a barrier? Can the emerging technology spread and move from low to high density zone smoothly like osmosis or reverse osmosis?

Technological innovation is closely associated with R&D policy and organizational learning strategies in new product development and process innovation. There are various strategies of learning such as learning-by-doing and learning-before-doing. Learning by doing is effective in semi-conductor manufacturing and bio-technology sectors which demand low level of theoretical and practical knowledge. On the other side, learning-before-doing is possible through various methods such as prototype testing, computer simulations, pilot production run and laboratory experiments. It is effective in chemical and metallurgical engineering where deep practical and theoretical knowledge can be achieved through laboratory experiments that model future commercial production experience.

Let us explore the role of deep analytics on technological innovation. It is interesting to analyze the impact of different learning strategies and timing of technology transfer on product development performance, process re-engineering and R&D cost of top technological innovations. It is important to compare the effectiveness of various types of learning strategies in terms of cost, quality and time. It is also critical to analyze the relationship between process innovation and learning curve in terms of dynamic cost reduction and improvements in yield. In case of learning-by-doing, it is possible to acquire knowledge of new process development in specific production environment. But, some knowledge may be lost when a new process is transferred to commercial production environment. It is also interesting to analyze the impact of dedicated process development facilities, geographic proximity

between R&D lab and production plant and the duplication of equipment between development and production facilities on practical implementation, speed and effectiveness of top technological innovations. It is essential to identify the critical success factors (e.g. resource allocation, ERP and SCM strategies) that influence the rate of learning and superior performance.

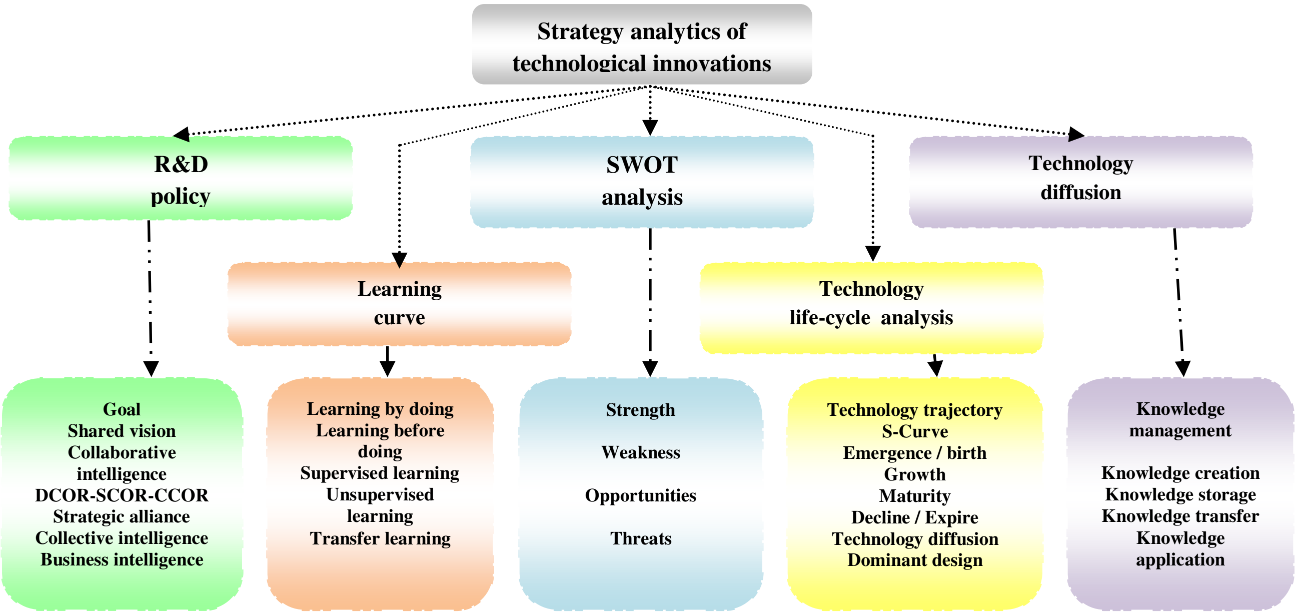


Figure 1.6: Strategy analytics

SWOT Analysis

Strength (High efficiency)	**Opportunities (Growth, Profit)**
Weakness (High Cost)	**Threats (Environmental pollution)**

Figure 1.7 : SWOT Analysis

It is rational to evaluate strength, weakness, opportunities and threats of a technological innovation [Figure 1.7]. There may be major and minor strengths and weaknesses. Strength indicates positive aspects, benefits and advantages of a strategic option. Weakness indicates negative aspects, limitations and disadvantages of that option. Opportunities indicate the areas of growth of market and industries from the perspective of profit. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses.

Technological life-cycle analysis **: Deep analytics evaluate and explores top technological innovations in terms of technology life-cycle, technology trajectory, S-**

curve, technology diffusion and dominant design. No element in this universe exists eternally. Similarly, each technology emerges, grows to some level of maturity and then declines and eventually expires [Figure 1.8]. It is essential to evaluate the status of each technological innovation through TLC analysis. Some technologies may have relatively long technology life-cycle; others never reach a maturity stage. Emergence of new technologies follows a complex nonlinear process. It is hard to understand how the technology life-cycle interacts with other technologies, systems, cultures, enterprise activities and impacts on society. All technologies evolve from their parents at birth or emergence phase; they interact with each other to form complex technological ecologies. The parents add their technological DNA which interacts to form the new development. A new technological development must be nurtured; many technologies perish before they are embedded in their environments. Next phase is growth; if a technology survives its early phases, it adapts and forwards to its intended environment with the emergence of competitors. This is a question of struggle for existence and survival for the fittest. Next phase is a stable maturity state with a set of incremental changes. At some point, all technologies reach a point of unstable maturity i.e. a strategic inflection point. The final stage is decline and phase out or expire; all technologies eventually decline and are phased out or expire at a substantial cost. TLC may have other different types of phases such as acquisition, utilization, and phase-out and disposal; preparation or initiation, implementation and operation; organization, directive, delegation, coordinate, collaborative, and dissolution; acquisition; emergence, diffusion, development and maturity.

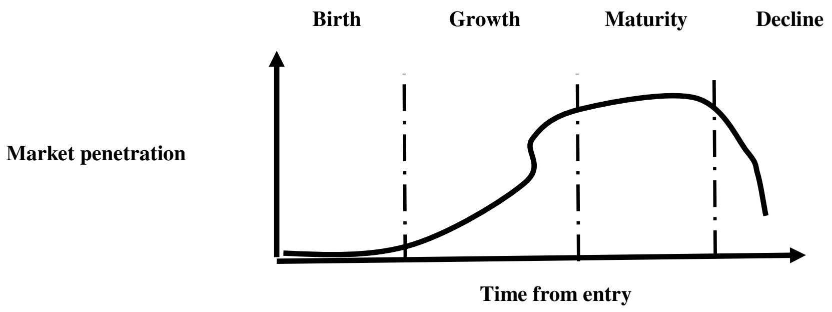


Figure 1.8 : Technology life–cycle analysis

Let us consider the analysis of the performance of a new technology vs. effort; it is basically S-curve. Initially, it is difficult and costly to improve the performance of a new technology. The performance begins to improve with better understanding of the fundamental principles and system architecture. Finally, the technology approaches its inherent limits with diminishing returns. Next, let us analyze the adoption of a new technology over time which is also an S curve. Initially, a new technology is costly for the adopters due to various uncertainties and risks. Gradually, this new technology is adopted by large segments of the market due to reduced cost and risks. Gradually, the diffusion of new technology slows with the saturation of market or due to the threats imposed by other new technologies.

The rate of improvement of a new technology is often faster than the rate of market demand over time; the market share increases with high performance. Technological change follows a cyclical pattern. The evolution of a technology passes through a phase of turbulence and uncertainty; various stakeholders of a supply chain explore different competing design options of the new technology and a dominant design emerges alongwih a consensus and convergence of structure. Then, the producers try to improve the efficiency and design of products based on stable benchmark of the industry. The dominant design considers an optimal set of most advanced technological features which meet the demand of the customer, supply and design chain in the best possible way.
Technology trajectory **is the path that a technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors and patterns of technology trajectories of top innovations today. How to manage evolution of technological innovation? The nature of innovation shifts markedly after a dominant design emerges. The pace of performance improvement utilizing a particular technological approach is expected to follow S-curve pattern. The evolution of innovation is determined by intersecting trajectories of performance demanded in the market vs. performance supplied by technologies. Technology diffusion indicates how new technologies spread through a population of potential adopters. It is controlled by characteristics of innovation, characteristics of social environment and characteristics of the adopters such as innovators, early adopters, early majority, late majority and laggards.**

Technology forecasting **: From the perspectives of technology management, the basic objectives of deep analytics involve integrated strategic planning, forecasting, design, optimization, operation and control of various technological products, processes and services to understand the dynamics of technology innovation, hype, priority, capability, maturity, adoption, diffusion, infusion, transfer, life-cycle, dominant design, spillover effects, blind spots and also the value of emerging technologies for our society. The basic objective of technology forecasting is to predict the future characteristics of emerging technologies for humanity (e.g. machines, procedures, speed, power, accuracy or precision) through a set of commonly adopted methods such as Delphi method, forecast by analogy, growth curves and extrapolation; may not have to state how these characteristics will be achieved. It is possible to combine two forecast methods (e.g. growth and trend curves) to offset the weaknesses of a method with the strengths of another method and to give the forecaster more insight.**

Dominant design **: Dominant design is a concept of technology management, identifies key technological features that become a de facto standard. The innovators must try to explore dominant design to win the market share. Dominant design may be a new technology, product or a set of key features as the outcome of a set of independent technological innovations. When a new technology emerges, different firms introduce a number of alternative designs based on incremental improvements. The dominant design enforces standardization, results economies of scale and competition starts based on cost, scale, product features and performance. Dominant design may not be better than other designs; simply incorporate a set of**

key features that emerge due to technological path-dependence and not necessarily strict customer preferences. Dominant designs are expected to acquire more than 50% of the market share. The process of dominance passes through a few milestones. An innovator conducts R&D to create a new product or service or improve an existing design. The first working prototype of emerging technology sends a signal to competitors to review the feasibility of their research programs. The first commercial product is launched and directed at a small group of customers and force the competitors to review and speed up their research efforts. A clear front runner emerges from the early market. Finally, a particular technological trajectory achieves dominance.

***Technology innovation*: What is diffusion innovation theory developed by E.M. Rogers (1962)? It explains how, over time, an idea or product gains momentum and diffuses or spreads through a specific population or social system. What is the difference between innovation and diffusion? Diffusion refers to the process by which innovations spread among the members of a social system over time in an organizations, adoption is a decision of implementing innovations based on knowledge, and persuasion of individuals within a given system. An organization seeks to improve efficiency through the adoption of innovative information and communication technologies such as better safety, competitive advantage, fewer errors, greater accuracy, higher quality products, improved communications, increased efficiency and productivity, efficient administration, and improved financial and managerial performance. What is product innovation and diffusion process? The diffusion of innovation is the process by which new products are adopted (or not) by their intended audiences. It allows designers and marketers to examine why it is that some inferior products are successful when some superior products are not. Why is diffusion of innovation important? Diffusion of innovation is responsible for the launch and spread of some of the most important advanced technologies in human history, What is technology absorption? It is the acquisition, development, assimilation and utilization of technological knowledge and capability by a firm from an external source; it occurs between transferring and receiving entities. What is technology innovation management? The basic objective is to train aspiring entrepreneurs on creating wealth at the early stages of a venture or opportunity life cycles; it focuses on the launch and growth of technology companies and growth seeking initiatives of existing companies.**

What is the diffusion of innovation curve? The diffusion of innovations curve (innovation adoption curve) of Rogers is useful to understand that trying to quickly and massively convince the mass of a new controversial idea is useless. It makes more sense in these circumstances to start with convincing innovators and early adopters first. What factors influence the rate of adoption and diffusion of innovations? There are specific products and service attributes that affect the diffusion process and can influence consumer acceptance of new products and services; these factors are relative advantage, compatibility, complexity, trialability, and observability. What is technology export? High-technology exports are products with high R&D intensity such as in aerospace, computers, pharmaceuticals, scientific instruments, and electrical machinery. What are the two advantages of technology management? The advantages of

new technology is that it allows companies to automate functions that previously required employees. Tasks like data entry and analytics, bookkeeping, and contact management can be partially or completely automated, which allows businesses to work more efficiently without the risk of human errors. How is technology transferred? Transfer of technology is the process of transferring or disseminating technology from the person or organization that owns or holds it to another person or organization, Horizontal transfer is the movement of technologies from one area to another. The diffusion of an innovation is the spread of a product, process, or idea perceived as new, through communication channels, among the members of a social system over time.

What are the disadvantages of a technology? The machines are becoming more intelligent, advanced and efficient and support innovation. The disadvantages are loss of job opportunities. Can we survive without technology? Yes, for most people, technology is not something we give a second thought but some people can't live without it For some people, the existence of technology is the difference between silence and laughter, loneliness and interaction and even life and death. How does a technology affect our life? Technology can affect life both positively and negatively. New technology always changes our life very much and takes it to a new level. It is like the new way of thinking or doing the normal things differently, better and much more faster with less hassle and at a much affordable rate.

***Technology diffusion* : Diffusion is a physical process that refers to the net movement of molecules from a region of high concentration to one of lower concentration. The material that diffuses may be a solid, liquid or gas. A drop of ink coloring diffuses throughout the water in a glass; the smell of perfume diffuses everywhere in a room. What is diffusion mechanism? The diffusion of a particular lattice atom by a vacancy mechanism is inextricably linked to the movements of vacancies, but is something different! Others are indirect interstitial mechanisms. What is the principle of diffusion? It is the movement of a component through space under the influence of a physical stimulus. The most common cause of diffusion is a concentration gradient which tends to adjust the component concentration until it reaches equilibrium. In short, diffusion is the physical flow of material. What is the difference between imbibition and diffusion? Imbibition is a reversible process whereas diffusion is an irreversible process. Imbibition is the absorption of water by general surface whereas diffusion is the movement of solid, liquid or gaseous molecules from the region of higher concentration to lower concentration. Can we explore the concept of technology osmosis?**

***Technology diffusion* is the process by which innovations of emerging technologies are adopted by a population. The rate of diffusion depends on several factors such as nature and quality of innovation, how information about the innovation is communicated and characteristics of the population into which the technology is introduced. Why is technology diffusion important? Technology diffusion plays a major role in most of the countries today. We can increase the trade by removing the diffusion barriers since the countries achieve higher productivity by taking the technology from the diffusion process. What is meant by technology diffusion? Technological diffusion is the process by which innovations (new products, new processes or new methods) spread within and across economies. What are the steps**

of diffusion? Diffusion occurs through a five step decision making process. It occurs through a series of communication channels over a period of time among the members of a similar social system. Rogers' five stages are awareness, interest, evaluation, trial, and adoption of technologies. What are the five adopter categories? Market researchers have classified consumers into five categories on the basis of their adoption of a product during different stages of that product's life cycle. The five adopter categories are innovators, early adopters, early majority, late majority and laggards. What are different diffusion strategies? The goal of any diffusion strategy is to spread the word about your innovation and encourage users to adopt it. These strategies may also be modified and used to target any other user group. What is rate of diffusion in technology management? Diffusion is the process by which a new idea or new product is accepted by the market. The rate of diffusion is the speed with which the new idea spreads from one consumer to the next.

***Technology adoption*: Within the rate of adoption, there is a point at which an innovation reaches critical mass. The categories of adopters are innovators, early adopters, early majority, late majority, and laggards. What is the difference between diffusion and adoption process? Diffusion is a macro process concerned with the spread of a new product from its source to the consuming public. Adoption is a micro process that focuses on the stages through which an individual consumer passes when deciding to accept or reject a new product. What is the late majority? Late majority refers to the second to last segment of a population to adopt an innovative technology. The late majority accounts for roughly 34% of the population and may adopt a new product only after seeing that the majority of the population already has successfully adopted it. What is diffusion and adoption of innovation? There are various strategies of technology adoption : align technology and strategy; communicate for buy-in and engagement; perform a current systems analysis; develop training approach early and integrate technology deployment with change management; create an effective governance structure. Technology diffusion is a measure of how widely technology is spread throughout an organization. *Technology infusion*, on the other hand, is the extent to which technology permeates an area or department. Technology infusion is the process of strategically binding technical needs and potential solutions.**

***Technology spillover effects*: A group of firms from emerging economies may enjoy unintentional technological benefits from R&D efforts of leading firms from advanced economies without any additional cost sharing. Successful technology spillovers depend on the absorptive capability of the receiving firms, technological gaps, interactions, information symmetry and knowledge flows between sending and receiving firms and also geographical and cultural proximity of a social process. Technology spillover is ultimately a learning experience for both sending and receiving firms. In economics, a spillover may be an economic event resulting positive or negative spillover effects. Negative spillover effects may occur when a market or economy suffers due to the slowdown in a different economy. For example, odors from a rendering plant or a flower garden are negative or positive spillover effects upon its neighbors. Spillover benefits are the opposite of spillover costs; the benefits that third parties or society receive from the actions of**

others. It may be considered as third party effect. For example, the economic benefits of increased trade are the spillover effects anticipated in the formation of strategic alliances (e.g. SAARC, ASEAN).

Strategy Analytics

Agents: System analysts, business analysts, technology management consultants;
Objects / entities: sustainable smart cities, smart villages, communities, smart world, smart universe;
Strategic moves :

- Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements – scope, system, structure, security, strategy, staff-resources, skill-style-support;
- Define a set of sustainable development goals and emerging technologies accordingly. /* Refer to scope and system analytics, sections 1 and 2 */
- Business model innovation
    - Who are the consumers?
    - What should be the offering of products and services?
    - What do the consumers value?
    - What is the revenue stream ?
    - How to deliver values to the consumers at rational cost?
- Define R&D policy : shared vision (refer : scope analytics, section 1), sustainable development goals, collaborative intelligence, collective intelligence, business intelligence;
- Do learning curve analysis – learning by doing, learning before doing;
- Do SWOT analysis – strength, weakness, opportunities, threats.
- Explore dominant design.
- Do technology life-cycle analysis and technology spillover effects.
- Explore technology innovation-adoption-diffusion strategy.
- Explore innovation model and knowledge management model for creation, storage, sharing and application of knowledge.
- Adopt '4E' approach : Envision, Explore, Exercise, and Extend.

Let us first explain the motivation of the problem on 'Business Analytics – Technology for Humanity'. We can consider a technology tree for the sustainable goal of human civilization based on security, global economic growth, generation of new job opportunities, elimination of poverty, business model innovation and the regulation of environmental pollution, global warming and climate change. Is it possible to ensure security of the people of the world from different perspectives such as physical safety from natural disasters and acts of terrorism, social security, financial security, food, garment, accommodation, education, healthcare, communication, culture, energy and utilities globally? We have selected a set of emerging technologies for sustainable goals : solar power, electrical and hybrid vehicles, solar computing, deep analytics, Adaptive security for Supervisory Control & Data Acquisition (SCADA) & Industrial Control System (ICS), railtech security & safety, cancer care : deep learning, precision medicine and genomics, biomedical technology for cancercare, artificial rainfall through cloud seeding, real-time

moving target search against astronomical hazards and digital technologies including secure adaptive filter and secure multiparty quantum computing, 5G-6G-7G-8G wireless communication technologies and cloud computing. With the significant advancement of information and communication technology, computing is perceived to be used as the next utility after water, electricity, gas and telecommunication. Session 15 has explored the classification of emerging digital technology through a technology tree. Digital technology is classified into communication and information technologies at level 1 of the technology tree. The scope of emerging communication technology is explored in terms of [cloud computing, cloud streaming, cloud analytics], [Internet of Things (IoT), Industrial IoT, edge computing], next generation wireless and mobile communication, broadcast and satellite communication, RFID and sensor networks at level 2. The scope of emerging information technology is explored in terms of [adaptive security, secure adaptive filter, dynamic data protection, cyber security, crash proof code]; [applied AI and machine learning, soft computing, deep learning, robotics]; [deep analytics, predictive analytics, collaborative analytics], virtual and augmented reality, digital twins, solar computing, pervasive computing, wearable computing, secure multiparty quantum computing and ray tracing.

In today's business environment of increasing globalization, rapid technological advancement and knowledge based economy, human capital should be considered as a strategic asset and a sustainable resource of competitive advantage in improving performance of a research organization. Intelligent analytics should be integrated with human resource information system (HRIS) for efficient, consistent and correct decision making of top management on various strategic issues of research and development of emerging technological innovations. Analytics is positively associated with decision taking on human resource management and can predict future workforce planning rationally. Deep analytics is the backbone of HRIS which uses information technologies to acquire, store, manipulate, analyze, retrieve and distribute strategic data for effective management of various HR functions such as workforce planning, employee benefits, administration, payroll, recruitment; induction, orientation and on-boarding, training and development, skills management, personnel administration, time management, travel management, personnel cost planning; and performance appraisal. Deep analytics is expected to combine people, information, skills, technologies, applications, and business processes to make better strategic and tactical decisions for the innovation, adoption and diffusion of emerging technologies for humanity. Intelligent multidimensional HR analytics should analyze the effectiveness of HR policy, talent acquisition and retention, skill development, incentives, reward and recognition through data visualization (e.g. reports, graphical charts, alerts, dashboards) and performance metrics).

Figure 10.1 shows the classification of emerging digital technology. This is an interesting example of technology association. Level 1 shows the classification of digital technology. Level 2 shows the technology association of various types of communication technologies such as cloud computing, cloud streaming, cloud analytics, IoT and IIoT. It is possible to explore the scope of digital technology

through Business Process Reengineering (BPR) approach (analyze as-is process and related IS, identify gaps and risks of as-is processes and IS and design to-be processes and system); top-down approach, critical success factor (CSF) analysis based on business objectives, constraints and requirements engineering, value chain analysis, bottom-up approach and inside-outside approach. The basic objective of this summit is to explore a set of fundamental questions on technology management.
***Scope*: What is technology swing? What is the scope of a technology innovation? What do we mean by *technology classification*? A *technology tree* shows the classification of technologies at various levels. For instance, it is possible to classify digital technology into communication and information technologies on the basis of computing, data, networking, application and security schema. The concept of technology classification will be explored during session 10. What do we mean by *technology association*: a set of technologies are closely associated with each other, A technology may grow with the advancement of its associated technologies. This book shows the technology association among solar power, electrical and hybrid vehicles and solar computing; another technology association has been found out among precision medicine, genomics, deep learning and biomedical technology for cancer care. We have also observed technology association among web technology, cloud computing, IoT and IIoT; adaptive security, dynamic data protection and secure multi-party computation. Please note that technology association is different from the traditional concept of technology forum. Rather it highlights the link, fit and dependencies among a set of technologies. The growth, maturity, innovation, adoption and diffusion of a technology depends on the advancement of the associated technologies. What do we mean by *technology clustering?* It indicates a cluster of technologies based on similarity. Each cluster of technologies are closely interrelated with each other. Another interesting issue is *technology forecasting*: is it possible to forecast the growth of an emerging technology using rational predictive analytics?**
Next critical element is *System:* What are the basic schema and dominant design of a system associated with a technology innovation? What is s*tructure; w*hat are the basic elements of the system architecture associated with an emerging technology? How to represent the structure correctly and transparently through multi-dimensional simulated modeling such as digital twins? Another important is security What do you mean by technology security? How to verify the security intelligence of a system associated with a technology innovation? Strategy plays an important role in technology complexity analysis: What are the strategic moves of technology innovation, adoption, diffusion and infusion? What is the outcome of technology life-cycle analysis? How to compare an emerging technology with the existing old technologies through SWOT analysis? What are the technology spillover effects? What are the blind spots and critical success factors? An important demand of an emerging technology is s*taff - resources*: how to exercise enterprise resource planning and supply chain management of a technology innovation project in terms of man, machine, material, method and money? What should be the talent management strategy? The final critical factor is s*kill-style-support*: what are the skills, leadership style and support demanded by a technological innovation? How to manage technology innovation projects efficiently

through resource and time constrained, stochastic, adaptive multi-objective and multimode project scheduling algorithms? What should be the shared vision, common goals and communication protocols? How to ensure a perfect fit among '7-S' elements? What type of organization structure is essential for various types of technology innovations? How to perform aforesaid analysis using statistical / quantitative tools? What types of tools are useful for technology management :

- **Technology forecasting**
    - **Prediction of technology failure**
    - **Prediction of technology success**
    - **Prediction of market share**
- **Technology clustering**
- **Technology classification**
- **Technology association : support and confidence**
- **Simulation : technology innovation, adoption, diffusion , infusion, trnsition**

The expert panel have adopted two approaches to develop '7-S' model of deep analytics for technological complexity analysis. The first approach is learning-before-doing. We have reviewed relevant literature on technology management and have defined an initial framework of deep analytics. We have reviewed on top emerging technologies today from the technical reports of Gartner, IEEE, MIT and other sources. We have observed that today, technology management demands a rational balanced approach for the benefits and sustainability of humanity globally. There is too much focus on information and communication technology; but less focus on other critical domains such as biomedical and electrical engineering, nanotechnology, earth and space science.

Next, we have selected a set of potential strategic technologies for humanity which have significant impact on our society globally. The most of these technologies are at emergence phase of TLC; the others are passing through growth phase. As a part of learning-by-doing approach; we have analyzed these emerging technologies for humanity using '7-S' model and have backtracked to redefine the initial framework of deep analytics.

Finally, let us consider a set of interesting queries. How to define 'Sustainable Development Goals' for the sustainability of human civilization? Should we focus on a set of path breaking technologies based on top most priorities? Is there too much focus on the innovation of digital technology (e.g. ICT) ignoring the basic necessities of life? Can AI and Robotics solve all the problems of our universe? We can not deny the progress of technology today but are we at the point of saturation in innovation or lot of works are still pending? "Miles to go before I sleep; Miles to go before I sleep". Can we fight against various types of natural disasters effectively such as flood, drought, earthquake, cyclone, storm, volcano and astronomical hazards effectively with existing technologies? Can we manage natural resources such as sunlight, wind, water, soil and others with existing technologies effectively? What should be the critical success factors to deploy technology for humanity effectively throughout the world : democracy, demography, demand, political stability and decisiveness of government? Isn't the act of terrorism and natural

disaster a real threat to humanity? Shouldn't we fight against terrorism for the sake of humanity? Shouldn't the world be united; how to ensure unity, harmony and peace through sustainable development goals? What should be the vision of global superpower and leadership for global welfare, cooperation and collaboration?

7. STAFF-RESOURCES

Dr. Moore is analyzing the sixth element of deep analytics - staff-resources in terms of 5M (man, machine, material, method and money). In today's business environment of increasing globalization, rapid technological advancement and knowledge based economy, human capital should be considered as a strategic asset and a sustainable resource of competitive advantage in improving performance of a research organization. Deep analytics should be integrated with human resource information system (HRIS) for intelligent, efficient, consistent and correct decision making of top management on various strategic issues of research and development of emerging technological innovations through data visualization tools (e.g. reports, graphical charts, dashboards, alerts and performance metrics).

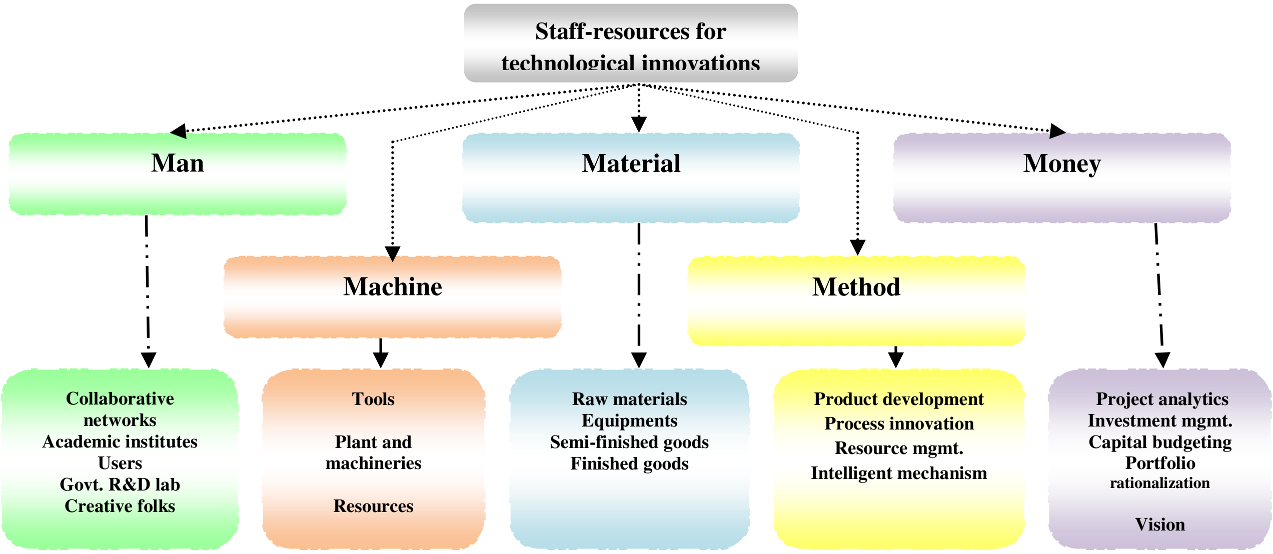


Figure 1.9 : Staff-resources analytics

Deep analytics is positively associated with decision taking on human resource management and can predict future workforce planning rationally. Deep analytics is the backbone of HRIS which uses information technologies to acquire, store, manipulate, analyze, retrieve and distribute strategic data for effective management of various HR functions such as workforce planning, employee benefits, administration, payroll, recruitment; induction, orientation and on-boarding, training and development, skills management, personnel administration, time management, travel management, personnel cost planning; and performance appraisal. Workforce planning should be done based on workforce demographic data, headcount development, turnover rates, workforce cost planning and

workforce composition. It is useful for headcount planning, budgeting, recruiting, learning and continuous monitoring of performance. Workforce process analytics analyzes the effectiveness of HR processes such as payroll, employee administration, time management, jobs and organizational structures, Talent management analytics highlights skills of human resources for innovation of emerging technologies and also strategic alignment. Deep analytics is expected to combine people, information, skills, technologies, applications and business processes to make better strategic and tactical decisions for the innovation, adoption and diffusion of emerging technologies for humanity.

'Man' **analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, payment function, compensation, reward, incentive and performance evaluation.** ***'Machine'*** **analyzes the basic aspects of tools and automated / semi-automated / manual machines;** ***'material'*** **analyzes planning of raw materials, equipments, semi-finished and finished goods.** ***'Method'*** **explores various aspects of process innovation, intelligent mechanism and procedure. Finally,** ***'money'*** **highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.**

It is crucial to analyze dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion such as 5M i.e. man, machine, material, method and money; dominant design factors, effects of timing and mode of entry. ***Method*** **is basically** ***process innovation*** **through process mapping : analyze as-is process; identify gaps and design to-be process. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment.**

Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. Some users or customers or clients or private nonprofit organizations may innovate new products or services based on their own needs. Many firms set up excellent R&D lab and also collaborative networks with customers, suppliers, academic institutes, competitors, government laboratories and nonprofit organizations. Many universities define sound research mission and vision and contribute through publication of research papers. Government also plays an active role in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators).

A complex technological innovation often needs ***collaborative intelligence*** **to manage the gap between demand and supply of a specific set of capabilities, skills and resources. It is possible to control cost, speed and competencies of technological innovations through efficient sharing mechanisms. It is rational to share the cost and risks of new innovations through creation, storage, transfer and application of knowledge among the partners of the innovation ecosystem. There are different modes of collaboration such as strategic alliance, joint ventures, technology licensing, outsourcing and collective research organizations.** ***Collaborative networks***

are other sources of innovation. Collaboration is facilitated by geographical proximity, regional technology clusters and technology spillovers. Technological spillover results from the spread of knowledge across organizational or regional boundaries; it occurs when the benefits from R&D activities of a firm spill over to other firms. But, it may be hard to control the development of product and process innovation protecting IP of proprietary technologies. The critical success factors of collaborative networks may be the right selection of innovation partners having strategic and resource fit, transparent and flexible monitoring and governance process so that the innovation partners understand their rights and obligations. .

Technological innovation demands the motivation and commitment of creative people. For example, the evolution of electronics and communication technology has been possible because of the involvement of the creative and efficient engineers and scientists in related domains. Most of top technology innovations are not trivial problems; need useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. The impact of knowledge on creativity is double-edged. Lack of knowledge is a major constraint to the original contribution in a technological innovation. But, extensive knowledge may be biased and trapped in existing logic and paradigms. It is difficult to conclude that moderate knowledge is adequate for creativity. A creative person is expected to have confidence in own capabilities, tolerance for ambiguity, interest in solving problems and willingness to overcome obstacles by taking reasonable risks. A cooperative and collaborative environment must recognize and reward creative talent in time. Organizational creativity is associated with several critical factors such as human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routines, performance evaluation, compensation, reward and incentive policy, social processes and contextual factors.

Resource Allocation Analytics : When the capacity of a firm is more than the total demand of a set of technological innovation projects, the resource manager may like to allocate the required resources such as fund or capital to each project using suitable resource allocation model. However, when the capacity is less than total demand, the resource manager would have to find the combination of projects, which would fit the resource allocation model and give maximum benefit. There are three different types of resource allocation protocols: linear, proportional and selective allocation.

***Linear allocation*: It is an equal sharing of the pain i.e. shortage of capacity of capital among a set of projects. If that pain exceeds the actual demand of a project, then the project becomes passive. The project P_i is allocated $q_i = d_i – (1/n) \max (0, \sum_{i=1}^{n} d^*_i - C)$ where n is the number of active projects, C is the capacity of capital of the client.**

***Proportional allocation* : The project P_i is allocated $q_i = \min\{d^*_i, C.d^*_i/(\sum_{i=1}^{n} d^*_i)\}$.**

Here, n is the number of active projects and C is the total capacity of capital of the client. If the demand is more, more capital will be allocated to that project proportionately.

***Selective allocation* : It is basically priority based portfolio rationalization where the capital is allocated as per the priority of a set of technological innovation projects. It is an interesting problem to find the allocation of the projects while maximizing the utility of the client under capacity constraints. This is basically a knapsack problem. Let $\{(u_1,d^*_1),(u_2,d^*_2), ..,(u_n,d^*_n), C\}$ be an instance of the *knapsack problem* – C is the knapsack capacity i.e. total capacity of capital of the client; (u_i,d^*_i) are respectively the utility and demand of capital of the project i. The goal is to choose a subset of projects of maximum utility with total demand of capital at most C. According to this resource capacity allocation strategy, all the projects are not treated equally. In case of any shortage of capacity, several projects may become infeasible. The projects are ranked based on utility and priority and the capital is allocated as per the rank of the projects.**

The business analysts should consider a *financial investment framework* for optimal resource allocation and project portfolio rationalization along two dimensions: strategic objective and technology scope [Figure 1.10]. There are four cells: transformation, experiments, process improvements and renewal. Most of the technology innovation projects fall in transformation and experiments cells. The basic objectives of transformation projects are growing need of application integration, end-to-end business process re-engineering and improved support. It demands process change. But, during economic downturn, it may be a costly option. The expected benefits are efficient customer service, greater accuracy and long-term growth. The basic objectives of experiments are to adopt new business models using new technology; the expected benefits are change of organization structure, infrastructure and business process improvements. The basic objective of process improvement is to yield more profit from improved operational performance. The process owner or a functional unit realizes benefits such as short term profitability. The basic objective of renewal is to replace old shared technology with new cost effective powerful technology maintaining the existing infrastructure and keeping it cost effective. The expected benefits are improved maintainability, reduced support and efficient capacity utilization.

***Resource allocation* and *mobilization* are two critical aspects of project management. It is possible to call different types of logic such as linear, proportional and selective resource allocation (as stated above) subject to shortage of capacity. Each strategic project defines a set of objectives, strategies and demand plans and then the resources are allocated to different projects according to the demand plans. It is basically the principle of *management by objectives (MBO)* which commits the reservation of different types of financial, non-financial and human resources. The sick projects may need new investment for turnaround and renewal; the star projects may need additional fund for continuous strategic growth; the emerging projects may need capital for appropriate technology management and skill development. The old dead assets should be divested; wastage of energy, utilities,**

materials and products should be minimized and existing capacity should be utilized intelligently.

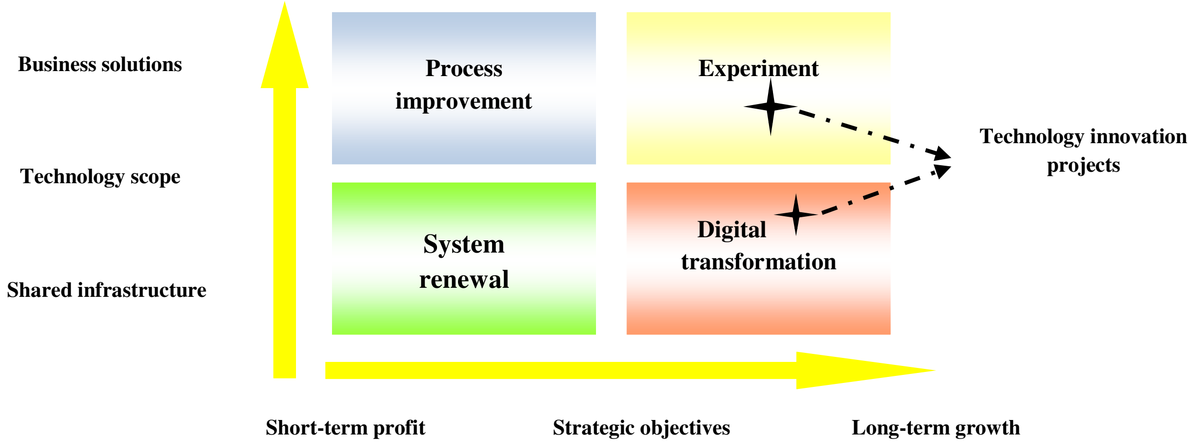


Figure 1.10 : Financial Investment Framework

The resources are generally allocated to different business units through various types of *budgeting* such as *capital budgeting*, *performance budgeting*, *zero based budgeting* and *strategic budgeting*. Capital budgeting is decided based on payback period, NPV, IRR and profitability index. Zero based budgeting evaluates the particular demand and need of each project. It involves identification of decisive projects, analysis of each decisive project, ranking of the demand of each project and then allocation of resources. Strategic budgeting asks a set of fundamental questions: What is the goal of a project in terms of performance and results? What are the key activities or tasks to be done to achieve the goal? The management should be cautious of the risk of resource allocation such as limited resource capacity, competition and past commitments.

Staff-resources Analytics

Objects / entities: sustainable smart cities, smart villages, communities, smart world, smart universe;
Global security parameters: define a set of sustainable development goals. /* refer to scope and system analytics in sections 1 and 2 */
Do estimation, planning , capacity utilization, allocation and distribution of '5M' resources.

- ✪ ***Man* (human capital management [scientists, engineers, consultants, business analysts, system analysts, project managers], talent acquisition, talent retention, training, reward and recognition);**
- ✪ ***Machine* (tools, machines, computer hardware, software, internet);**
- ✪ ***Material* (raw materials, components, equipments, semi-finished, finished and outsourced goods)**
- ✪ ***Method* (process innovation, product development, R&D);**

- ✪ *Money* **(optimal fund allocation, project portfolio management, investment management, capital budgeting)**

8. SKILL-STYLE-SUPPORT

Prof. Nil Bajjio and Prof. Som are analyzing the seventh element of deep analytics is *skill-style-support* [Figure 1.11]. The workforce involved in top technological innovations are expected to develop different types of skills in technical, management and medical science domain such as research and development, knowledge management, new product development, process innovation, team management, design, protection of innovation, project management, supply chain management, sales and marketing, event management, construction, erection, testing, commissioning, product and service maintenance. The *intellectual rights* of technological innovations are protected through patents, trademarks, trade secrets and copyrights. The diffusion of the new technological innovation depends on the skills and capabilities of a group of firms in production, promotion and distribution of the new products and services globally.

The system administrators must have *leadership* skills in smart thinking, communication, coordination and change management. The workforce should develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The life-cycle of a technological innovation also depends on the intelligence of marketing strategies such as branding, promotion, advertising, launching time, pricing mechanism, product quality, profit margin, compatibility and market share. It is important to analyze market segmentation, cost of advertising and promotion, reach, information content and duration of exposure.

The diffusion of top technology innovations needs the *support* of great leadership style; they are not only industry leaders but also political one. The *style* is basically the quality of leadership; the great leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. The leaders must be able to share a rational vision; mission and values related to top technology innovations among all the stakeholders honestly and appropriately in time. It is really challenging for the great leaders to implement top technological innovations physically and practically in the form of commercial products and services. They have to face and tackle threats from traditional industries. Top management must tackle the complexity of system implementation by developing a dedicated project team, a right mix of committed resources and talents like technical and business experts.

What should be the right *organization model* for top technological innovations? A traditional functionally centered organization model may not be suitable for supporting end-to-end business processes. Such process management is more than a way to improve the performance of individual processes; it is a way to operate and manage a business. An enterprise that has institutionalized process management and aligned management systems to support is a process enterprise. It is centered on its customers, managed around its processes and is aligned around a common,

customer oriented goal. The business models of top technological innovations require the support of a process enterprise structure enabled with advanced information and communication technology. The structure should have project, design, production, supply chain management maintenance, human resource management, sales & marketing and finance cells. The structure should be governed by an executive committee comprising of CEO and directors. The process managers should be able to identify core processes in the value chain; communicate throughout the organization about these critical processes; create and deploy measures regarding end-to-end process performance and define process owners with end-to-end authority for process design, resource procurement, process monitoring for redesign and improvement. The structure of process enterprise requires a collaborative and cooperative work culture. Top innovations need proactive, reactive and preventive support for proper technology management.

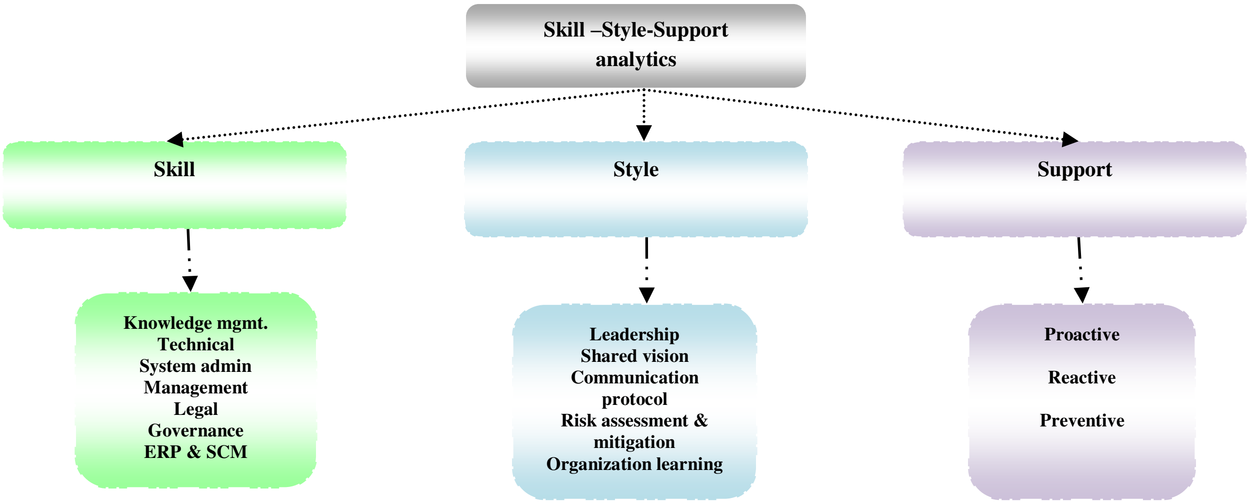


Figure 1.11: Skill-style-support analytics

***Innovation Model* : What should be the innovation model for effective diffusion of emerging technology? Is it possible to adopt *K-A-B-C-D-E-T-F model*? The model is associated with following stakeholders.**

- ***Knowledge manager*: The innovators should acquire the basic and fundamental concept through a *differentiated* course work; classify the primary, secondary and tertiary focus areas. Mandatory courses: Innovation, creativity and research methodology; communication. The depth and breadth of the course works should be traded off rationally. It needs proper guidance.**
- ***Activator*: The activators should initiate the innovation process by identifying a good research problem through scope analysis. Random selection of research problem should be avoided by evaluating the strength, experience and skill of the innovators. The research problem should have potential business intelligence and social benefits.**

- ***Browser***: **The browsers should search for information; investigate throughout the process and find relevant data or information to start innovation. They may review and analyze the existing works through traditional sources of research data (e.g. digital library, books, papers, journals, magazines, industry reports, you tubes) and also through webinars, social networking and attending seminars, workshops and conferences. Random search may result wastage of time; a systematic and planned / guided search process may lead to good results.**
- ***Creator***: **The creators should analyze the gap and think of to-be system; generate new ideas, concepts and possibilities and search for new solutions.**
- ***Developer***: **The developers should transform the ideas of the creation phase into good solutions; turn the ideas into deliverables, products and services. They should collaborate with different research forums, industries and experts during this phase.**
- ***Executor***: **The executors should implement and execute the roadmap of the innovation.**
- ***Tester:*** **The testers should do various types of experiments and laboratory works; verify system dynamics and monitor the performance of the deliverables. Advanced research laboratories are required for complicated testing and experiments.**
- ***Facilitator***: **The facilitators should define project plan, corporate governance policy, marketing plan, production plan, investment plan and cost-benefit analysis. They should be able to identify the revenue and profit making stream and fair, rational business intelligence. The government should provide financial assistance to the innovators in patent registration.**

Project Management Skill & Style

Traditional approaches to *project management* focus on long-term planning and stability to mitigate various risks. But, complex technology innovation project management needs a mix of traditional and agile approaches to cope with uncertainties. The intension driven role develops collaboration. The event driven role integrates planning and review with learning. The other important roles of the project managers are to prevent major disruptions and maintaining forward momentum continuously. They must acknowledge the emergence of a problem and then try to minimize the frequency and negative impact of unexpected events in a dynamic environment. They must be people, information and action oriented.

Traditional project management approach follows four steps such as definition, planning, execution and termination. But, no projects are so linear. Once project execution starts, reality may demand exception management i.e. the adjustment and amendment in the planning or definition phases. Each industry has a different profile of risk. Deep analytics is applicable to both adaptive and linear project management approaches for technology innovation. Many projects fail due to conventional approach which may not adapt to a dynamic business environment. It is very crucial to identify the *scope* of a project rationally through feasibility study and cost-benefit analysis. It is essential to identify the primary and secondary scopes through portfolio rationalization and analysis of priority, novelty, objectives and

constraints of a set of projects. Perception based emotional and readymade thoughts may affect the correctness of scope analysis. *Scope creep* is a serious concern in project management. It is not a simple task to tackle uncertainties and complexities in time and resource constrained project management for top technological innovations.

***Novelty* indicates how intensely new innovations are crucial aspects of a project. A project should be assessed on the scale of sophistication of technology, which may be low, medium or high. Another critical factor is the complexity of the project in terms of product, service and process. *Pace* indicates the urgency of a project which may be normal, fast, time critical or blitz. Different projects have varying degrees of newness or novelty. A derivative product development project may have low risk and few future concerns. The new version of an existing product needs detailed analysis and market research.**

Breakthrough product development projects face high risks. Each project is unique, but not in every respect and may have some common features. The uncertainty in a project is a measure of the mix of new and mature technology and existing knowledge base; it may arise from technological aspects, new service offering or new market segments. High technology projects are subject to time delays, cost overruns and risks of product failure. The complexity base measures three different types of complications within a project such as assembly (low), system (medium) and array (high). High complexity requires efficient coordination and integration among various phases and systems of a project. Pace indicates a sense of urgency and time sensitivity. The failure of time critical projects results from the violation of milestone deadlines and related opportunity loss; blitz projects are crisis projects with extremely urgent timing. There are various strategies for optimal pace management such as contingency plans, alternative solutions in parallel, resilient approach and business cases to manage emergency and to overcome uncertainties and unexpected surprises.

A technology innovation project may be delivered on time and budget through the efforts, skill and professionalism of the project managers. But, it may not meet the needs of the end customers due to uncertainty and misunderstanding. The basic objective of the deep analytics is to figure out the actual structure of a project as compared with the existing capabilities, the gap and the measure of project success in terms of efficiency, impact on the customer, impact on the team, business success and preparation for the future. It is rational to take both short and long term view of a project plan since success may change during the life-cycle of a project with the change of environmental parameters and information. Does anything change from a future point of view? Does a project have sufficient flexibility to adapt to new requirements of a dynamic business environment? Are the incentives aligned properly with customer satisfaction, system performance, deadline and budget requirements? The deep analytics is useful to find the gaps between as-is and to-be requirements of a project, efficient resource planning, uncertainty and risk management. Correct use of deep analytics clearly highlights low-medium-high benefit opportunity and low-medium-high risk difficulty.

The feasibility and opportunities of a technology innovation project are estimated through real option, DEA, net present value (NPV) or internal rate of return (IRR).

But, it is hard to compute discounted cash flows due to inherent risks and uncertainties associated with an innovation of new technology. Data envelopment analysis combines qualitative and quantitative measures; it is basically a multi-criteria decision making approach.

Project Analytics **: Classical models of resource constrained project scheduling problems are not adequate to solve real world problems due to increased complexities and uncertainties. Intelligent project analytics are essential for complex, fuzzy, stochastic, multi-mode, time and resource constrained project scheduling problems with multiple objectives. This work explores how to apply the concept of intelligent deep analytics for project management. Efficient project management requires coordination and integration among various elements. It is essential to define the scope of a project correctly through feasibility study, priority and cost-benefit analysis. It is a common practice to launch new projects with fake promises before an election. The society should be alert of such corruption.**

Project Performance: KPIs and Data Visualization Strategy: **It is essential for an efficient project manager to understand critical metrics and key performance indicators (KPI) and how to identify, measure, analyze, report and manage for the success of a project. KPIs and metrics are displayed in dashboards, scorecards and reports. Project metric is generic but KPI is specific. KPIs give early warning signs of poor project performance if the problems are not addressed appropriately. The project success is measured in terms of time, cost, performance and customer satisfaction. It is difficult to measure and monitor too many project performance metrics. Therefore, it is essential to consider optimal number of performance metrics and KPIs. It is possible to classify the performance metrics and KPIs into four categories.**
Category 1 [Operation] **: scope creep, project completion stage, flexibility, quality, cost, time, inventory, customer satisfaction; this category is associated with project success and element S_2 and S_3.**
Category 2 [Finance] **: revenue growth rate, cost reduction, profitability, ROI, payback period, NPV; this category is associated with element S_3.**
Category 3 [Human Resources (HR)] **: performance, productivity, capacity utilization, skill; this category is associated with element S_3.**
Category 4 [Security intelligence] : **It is essential to audit fairness and correctness (i.e. accuracy of estimate and measurement) of project plan computation and adjustment as per exceptions based on rationality.**

Skill-style-support Analytics

Objects / entities: sustainable smart cities, smart villages, communities, smart world, smart universe;
Global security parameters: define a set of sustainable development goals. /* refer to scope and system analytics in sections 1 and 2 */
Skill: Knowledge mgmt. Technical , System admin, Management, Legal, Governance, ERP & SCM

Style : Leadership, Shared vision, Communication protocol, Risk assessment & mitigation, Organization learning ;
Support : Proactive, preventive and reactive support, system maintenance,

9. OPEN AGENDA

The expert panel have found out several open research agendas on aforesaid deep analytics and '7-S' model:

- **Should We consider any additional elements for the proposed deep analytics which can streamline the evolution and diffusions of various technological innovations effectively? For instance the deep analytics may be 10-S model instead of 7-S in figure 1.1.**
- **Is it practically manageable to consider too many elements simultaneously? Should we consider resources instead of staff-resources? Should we decompose sixth element into skill, style and support separately? Should we position the element 'system' centrally or 'strategy' in figure 1.1?**
- **There are $^7C_2$ links (such as S1-S7, S2-S7,S3-S7,S4-S7, S5-S7, S6-S7....) among 7-S elements of the deep analytics; what are the implications of these links on complex technological innovations? There may be other various types of links considering $^7C_3$,$^7C_4$,$^7C_5$ and $^7C_6$ combinations (S1-S2-S3, S4-S5-S6-S7 ....).**
- **How do these elements of deep analytics impact technological innovation in terms of technology trajectory, spillover, dominant design and organizational learning process?**
- **How to foster creativity, problem solving capability, learning rate, generalizability, convergence and stopping criteria in organizational learning?**
- **What are the major constraints and barriers against the innovation, adoption and diffusion of technologies for humanity? There are several open issues of debate on the concept of deep analytics. It is an interesting observation from this book that we are living in 21st century today; but we could not reach the point of saturation of technology management at present; extensive R&D efforts are still pending for the sustainability of human civilization in the coming future.**

FURTHER READING

- **P. Attewell. 1992. Technology diffusion and organizational learning: the case of business computing, Organ. Sci., 3(1).**
- **Basalla, G. 1988. The Evolution of Technology, Cambridge University Press, New York.**
- **E.M. Rogers. 1995. Diffusion of Innovations, 4th ed., Free Press, New York.**

- M.W. Cardullo.1996. Introduction to Managing Technology, Vol. 4, J. A. Brandon, ed., Engineering Management Series, Research Studies Press, Taunton, England.
- D.I. Cleland and W.R. King. 1983. Systems Analysis and Project Management, McGraw-Hill, New York.
- N.W. Hatch and D.C.Mowery. 1996. Process Innovation and Learning by Doing in Semiconductor Manufacturing. Research policy, 25, 1097-1119.
- G. P. Pisano. 1996. Learning-before-doing in the development of new process technology. USA .
- W.B.Hirschmann. 1964. Profit from the learning curve. Harvard Business Review. 42(1)125-139,
- M. Kilbridge, M. 1962. A model for industrial learning. Management Sci. 8.
- G.P. Pisano. 1997. The Development Factory: Unlocking the Potential of Process Innovation. Harvard Business School Press, Boston, Massachusetts.
- M.E.Porter. 1980. Competitive Strategy. Free Press, New York.
- J.D.Teece, G, Pisano and A. Shuen. 1997. Dynamic capabilities and strategic management. Strategic Management . 18(7) 509-533.
- P.Adler and K. Clark. 1991. Behind the learning curve. Management Science 37(3), 267-281.
- K.Ulrich and S. Eppinger. 1995. Product Design and Development. McGraw-Hill, New York.
- E.Hippel and M. Tyre. 1995, How the 'learning by doing' is done: problem identification in novel process equipment. Research Policy 24(1), 1-12.
- Richard C. Dorf (Ed.).2000. Technology Management Handbook. Boca Raton: CRC Press.
- R. Adner. 2006. Match Your Innovation Strategy to Your Innovation Ecosystem. Harvard Business Review. April.
- R. Adner. 2002. When are technologies disruptive: a demand-based view of the emergence of competition. Strategic Management Journal 23(8): 667–688.
- R. Adner and D. Levinthal D. 2001. Demand heterogeneity and technology evolution: implication for product and process innovation. Management Science 47(5):611–628.
- R. Adner and P.Zemsky. 2002. Strategy dynamics through a demand-based lens: the evolution of market boundaries, resource rents, and competitive positions. INSEAD working paper series 2003/01/SM.
- R.Adner and P.Zemsky. 2005. Disruptive technology and the emergence of competition. Rand Journal of Economics 36(2): 229–254.
- J.M.Utterback and W. Abernathy. 1975. A dynamic model of process and product innovation. Omega 3(6):639–656.
- B. Wernerfelt. 1984. A resource-based view of the firm. Strategic Management Journal 5(2): 171–180.
- M.A.Schilling. 2017. Strategic management of technological innovation. McGraw-Hill Education.

- **M.A.Schilling. 2015. Towards dynamic efficiency: Innovation and its implications for antitrust Antitrust Bulletin.**
- **M. A. Schilling and C. E. Vasco. Product and Process Technological Change and the Adoption of Modular Organizational Forms. in Winning Strategies in a Deconstructing World, eds. R. Bresser,M. Hitt, R. Nixon, and D. Heuskel (Sussex, England: John Wiley & Sons, 2000), pp. 25–50.**
- **H. A. Simon. 1973. Technology and Environment. Management Science 19 (1973), pp. 1110–21.**
- **H. Chesbrough. 2003. Open Innovation: The New Imperative for Creating and Profiting from Technology, Harvard University Press, Boston.**
- **M.A.Schilling and C.Phelps. 2007. Interfirm Collaboration Networks: The impact of Large-scale Network Structure on Firm Innovation. Management Science 53, pp. 1113–1126.**
- **M. Boden. 1992. The Creative Mind: Myths and Mechanisms. New York: Basic Books, 1992.**
- **R. J. Thomas. 1995. New Product Success Stories: Lessons from Leading Innovators , John Wiley & Sons, NY.**
- **E. Roberts. 2001. Benchmarking Global Strategic Management of Technology. Research Technology Management, March–April, pp. 25–36.**
- **M. Dodgson. 2000. The Management of Technological Innovation. Oxford University Press, NY.**
- **A.B. Jaffe. 1986. Technological Opportunity and Spillovers of R&D: Evidence from Firms' Patents, Profits and Market Value. American Economic Review 76, pp. 984–1001.**
- **J. Sterman. 1983. Economic vulnerability and the energy transition, Energy Systems and Policy 7(4), 259-301.**
- **J.Sterman and J. Wittenberg. 1989. Path dependence, competition, and succession in the Stewart, I., Does God Play Dice? The Mathematics of Chaos. Cambridge, MA: dynamics of scientific revolution, Organization Science 10(3), 322-341**
- **J.W.Forrester. 1985. The model versus a modeling process, System Dynamics Review 1(1), 133-134.**
- **J.W. Forrester. 1968. Principles of systems. MIT Press, Cambridge.**
- **D. Kim and P. Senge. 1994. Putting systems thinking into practice, System Dynamics Review lO(2-3), 277-290.**
- **P. Senge. 1990. The Fifth Discipline: The Art and Practice of the Learning Organization. New York Doubleday.**
- **P. Senge and J. Sterman. 1992. Systems thinking and organizational learning: Acting locally and thinking globally in the organization of the future, European Journal of Operational Research 59(1), 137-150. (eds.) (1994) Modeling for Learning Organizations. Portland, OR: Productivity Press.**
- **P.K.J. Mohapatra and P. Mandal. 1989. System dynamics paradigm, Decision, 16(no. 4):251-266.**

- **A. E. Plaza. 1994. Case-based reasoning: foundational issues, methodological variations and system approaches, AI Communication. 7 (1), March, 39–59.**
- **D.B. Leake (Ed.). 1996. Case-Based Reasoning, MIT Press, Cambridge, MA, 1996.**
- **T.W.Malone, R.Laubacher and C.Dellarocas. 2010. The Collective Intelligence Genome. MIT Sloan Management Review. Spring, volume 51, no. 3.**
- **S.L.Epstein. 2015. Wanted : Collaborative Intelligence. Artificial Intelligence 221, 2015, 36 - 45.**
- **Averbakh. 2010. Nash equilibria in competitive project scheduling. European Journal of Operational Research 205, 552–556.**
- **W.Herroelen and R.Leus. 2005. Project scheduling under uncertainty: survey and research potentials. European Journal of Operational Research, 165, 289–306.**
- **A.J.Shenhar. 2001. One size does not fit all projects : exploring classical contingency domains. Management Science. Vol. 47 no. 3, pp. 394 - 414. March.**
- **H.Kerzner and C. Belack.2010. Managing Complex Projects, John Wiley & Sons and the International Institute for Learning (IIL) Co-publishers.**
- **H.Kerzner, 2006. Project Management Best Practices; Achieving Global Excellence, Hoboken, NJ:John Wiley & Sons Publishers.**
- **J.W.Ross and C.M.Beath. 2002. Beyond the business case: new approaches to IT investment. MIT Sloan Management Review. Winter.**
- **R.H.Waterman, T.J.Peters and J.R. Phillips. 1980. Structure is not organization. Business Horizons. June.**
- **S. Chakraborty and S.K. Sharma. 2007. Enterprise Resource Planning: An Integrated Strategic Framework. International Journal of Management and Enterprise Development, Volume 4, No. 5.**
- **B.E. Becker and M.A. Huselid. 2006. Strategic human resource management: Where do we go from here? Journal of Management 32(6), 898–925 (2006).**
- **A. Mishra and I. Akman, 2010. nformation Technology in Human Resource Management: An Empirical Assessment. Public: Personnel Management 39(3), 271–290.**
- **N.Kashive. 2011, N.: Managing Today's Workforce: Human Resource Information System (HRIS), Its challenge and Opportunities. International Journal of Research in Finance & Marketing 1(6), 38–66.**
- **T.S.Teo, G.S. Lim and S.A.Fedric. 2007. The adoption and diffusion of human resources information systems in Singapore. Asia Pacific Journal of Human Resources 45(1), 44–61.**
- **M,.G. Martinsons. 1994. Benchmarking human resource information systems in Canada and and Hong Kong. Information and Management 26(6), 305–316.**
- **Sachs, J., Schmidt-Traub, G., Kroll, C., Lafortune, G., Fuller, G. (2019): Sustainable Development Report 2019. New York: Bertelsmann Stiftung and Sustainable Development Solutions Network (SDSN)**

- **dpicampaigns. "About the Sustainable Development Goals". United Nations Sustainable Development.**
- **"United Nations Official Document". www.un.org.**
- **"Transforming our world: the 2030 Agenda for Sustainable Development". United Nations – Sustainable Development knowledge platform. UN2030 agenda (adopted at UN Summit in New York on 25-27 September 2015) by 2030 as per UN Resolution 70/1, 2030 agenda.**
- **"Global Goals | Policy and advocacy". Sightsavers. 25 September 2017.**
- **"17Goals – The SDG Tracker: Charts, graphs and data at your fingertips". Retrieved 10 March 2019.**
- **"The History of Sustainable Development in the United Nations". Rio+20 UN Conference on Sustainable Development. UN. 20–22 June 2012.**
- **Development, World Commission on Environment and. "Our Common Future, Session 2: Towards Sustainable Development - A/42/427 Annex, Session 2 - UN Documents: Gathering a body of global agreements". www.un-documents.net. 2017.**
- **"World leaders adopt Sustainable Development Goals". United Nations Development Programme.**
- **"Extreme poverty is falling: How is poverty changing for higher poverty lines?". Our World in Data.**
- **Ortiz-Ospina, Esteban; Roser, Max (25 May 2013). "Global Extreme Poverty". Our World in Data.**
- **Fan, Shenggen and Polman, Paul. 2014. An ambitious development goal: Ending hunger and undernutrition by 2025. In 2013 Global food policy report. Eds. Marble, Andrew and Fritschel, Heidi. Session 2. Pp 15-28. Washington, D.C.: International Food Policy Research Institute (IFPRI).**
- **WHO and UNICEF (2017) Progress on Drinking Water, Sanitation and Hygiene: 2017 Update and SDG Baselines. Geneva: World Health Organization (WHO) and the United Nations Children's Fund (UNICEF), 2017.**
- **Staples, D., & Hermes, R. (2012). Marine biodiversity and resource management – what is the link? Aquatic Ecosystem Health & Management, 15(3), 245–252. doi:10.1080/14634988.2012.709429**
- **Vierros, M. (2017). Global Marine Governance and Oceans Management for the Achievement of SDG 14. UN Chronicle, 54(1/2), 1.**
- **Metcalfe, K., Collins, T., Abernethy, K. E., Boumba, R., Dengui, J., Miyalou, R., … Godley, B. J. (2017). Addressing Uncertainty in Marine Resource Management; Combining Community Engagement and Tracking Technology to Characterize Human Behavior. Conservation Letters, 10(4), 459–469. doi:10.1111/conl.12293.**
- **van Putten, I. E., Plagányi, É. E., Booth, K., Cvitanovic, C., Kelly, R., Punt, A. E., & Richards, S. A. (2018). A framework for incorporating sense of place into the management of marine systems. Ecology & Society, 23(4), 42–65. doi:10.5751/ES-10504-230404**

- **Hughes, Z. D., Fenichel, E. P., & Gerber, L. R. (2011). The Potential Impact of Labor Choices on the Efficacy of Marine Conservation Strategies. PLoS ONE, 6(8), 1–10. doi:10.1371/journal.pone.0023722**
- **Finkl, C. W., & Makowski, C. (2010). Increasing sustainability of coastal management by merging monitored marine environments with inventoried shelf resources. International Journal of Environmental Studies, 67(6), 861–870. doi:10.1080/00207230902916786**
- **Bhargava, A. (2019). "Climate change, demographic pressures and global sustainability", Economics and Human Biology, 33, 149–154.**
- **Firzli, Nicolas. "Smart Capital and Sustainable Finance in the Sino-American Century", 16 December 2019, Private Debt Investor.**
- **Lietaer, Bernard (2019). "Towards a sustainable world - 3 paradigms to achieve", available as of Oct.31, 2019 ISBN 978-3-200-06527-7. Discusses "the law of sustainability" presented with Robert E.Ulanowicz and Sally J.Goerner.**
- **Wilson, Clive (2018). "Designing the Purposeful World - the Sustainable Development Goals as a blueprint for humanity" Routledge.**

Quiz

- **What is the technology swing and the scope of technology innovation? How can you define the goal of an emerging technology?**
- **What is the dominant design of this technology innovation?**
- **What are the basic elements of the system architecture associated with the technology innovation? How to represent the structure correctly?**
- **What do you mean by technology_security? How to verify the security intelligence?**
- **What are the strategic moves of technology diffusion?**
    - **What is the outcome of technology life-cycle analysis?**
    - **How to compare an emerging technology with the existing old technologies through SWOT analysis?**
    - **What are the technology spillover effects?**
    - **What are the blind spots and critical success factors?**
- **How do you estimate resource allocation for emerging technology management? What should be the talent management strategy? What do you mean by process innovation?**
- **What are the skills, leadership style and support demanded by a technological innovation?**
- **How to manage technology innovation projects efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How to ensure a perfect fit among '7-S' elements?**
- **What type of organization structure is essential for various types of technology innovations?**

- Can You think of any additional elements for the proposed deep analytics which can streamline the evolution and diffusions of various technological innovations effectively? Is it practically manageable to consider too many elements simultaneously? Is it appropriate to consider resources instead of staff-resources? Is it rational to decompose sixth element into skill, style and support separately? Can You validate to position the element ‘system’ or ‘strategy’ centrally in 1.1?
- There are $^{7}C_{2}$ links (such as S1-S7, S2-S7,S3-S7,S4-S7, S5-S7, S6-S7....) among 7-S elements of the deep analytics; what are the implications of these links on complex technological innovation, adoption and diffusions?
- There may be other various types of links considering $^{7}C_{3}$,$^{7}C_{4}$,$^{7}C_{5}$ and $^{7}C_{6}$ combinations (S1-S2-S3, S4-S5-S6-S7 ....). Can you explore any interrelationship among these different combinations of elements?
- Please study the following case and analyze ‘support’ element of deep analytics. It is a real case; the names of the company and customer have been changed to preserve the privacy of the entities.

“
From: A chakraborty
Sent: Thursday, October 24, 2019 5:44 AM
To: customer.connect@oorientelectric.com
CC: akashelectricalitsamiteshrai@gmail.com
Subject: Quality problem of Oorient fan – C-19102400203
To,
The Manager (Customer Care),
Oorient Electric Limited, 240, Hokhla Industrial Estate, Phase – III, New Belhi – 210020, Imdia
Email – customer.connect@oorientelectric.com
CC: Prakash Electricals, P-37, India Exchange Place, Kolkata -1; Email : akashelectricals@gmail.com; contact – 3986-1593 / 50241593
Subject : Quality problem of Oorient fan - C19102400203
Invoice no. : PI/9446, 30.7.2019
Customer complaint reference : C-19102400203, 24.10.2019
Product / item : 16” Oorient stand 37 Trendzz fan
Respected Sir,

I purchased an Oorient fan of the aforesaid model on 30.7.2019 from Akash Electricals, Koolkata. Last one month, I have been experiencing a problem related to the fan about 10 times. After running sometime, the fan has been getting off automatically. Again, the fan start rotating automatically after sometime.

I don’t know whether this is the problem of heating of motor of the fan. Today, I called Customer helpline no. 18001037575 and lodged a complaint. Previously, I informed but your service staff did not come in time (complaint ref.: 419073001645). Request you to take necessary corrective actions on immediate basis. I do not expect such type of quality problem from Oorient product.

Regards.
Amit Chakraborty

37/1, Mukherjee Bagan Lane, Balkia, Cowrah – 711106, Nest Bengal
Mobile : 4940433441

Email 2
Feedback : Quality problem of Oorient fan – C-19102400203
achakraborty 2013@hotmail.com Fri 10/25/2019 3:56 PM
To: customer.connect@oorientelectric.com
Cc: akashelectricals@gmail.com; sec.cad-wb@nic.im secy-ca@nic.im; cimoffice@nic.im; connect@mygov.nic.im
My reference : E-mail dated 24.10.2019

To, The Manager (Customer Care),Oorient Electric Limited,
Email – customer.connect@oorientelectric.com
CC: Akash Electricals, P-37, Imdia Exchange Place, Koolkata -1
CC: Ministry of Consumer Affairs; Govt. of Imdia.
Respected Sir,
Your service technician, Mr. S. Mandal (Mobile no. 9230040544) visited my place around 16-00 today and serviced the Oorient fan against the aforesaid complaint. I have following feedback to You on this service.
1. The service technician replaced the coil of my new fan with another coil he brought. He diagnosed that the coil of the motor of my Trendzz fan is malfunctioning. Is it a good quality of product which is malfunctioning within 3 months of purchase from an authorized Oorient dealer in Koolkata?
2. I don't know the details of the spare parts i.e. the details of the replaced coil: is it a new coil suitable for Oorient stand 37 Trendzz fan? I don't think so. The coil looks old and the color of the paint is missing at some places. I think, the coil is of a table fan, not of stand Trendzz model.
3. The service technician collected the xerox copy of the invoice and warranty card but did not sign the details of this service anywhere on my warranty card or any service document. He has not given me any document stating the details of spare parts replaced.
I do not know what should be the feedback of the aforesaid service – excellent, good or poor. It depends on the product life cycle of the fan. The demand of the consumers is shrinking due to quality problems of products and related service issues in our country today.
Regards.
Amit Chakraborty
"

- **Define global security policy based on a set of sustainable development goals. What are the goals to protect our planet?**
- **Define technology for humanity. Select a set of emerging technologies to ensure global security policy.**
- **Please study the following case study. Discuss the role of technologies to regulate poverty and to achieve social, financial and physical security of human society globally.**

Case Study: Poverty, Intrusion and Enterprise Resource Planning

Let us look at the problem of poverty of a group of neighboring countries: I, B, P, N, S and C. The ministries of finance and economic affairs, home, defense and foreign affairs of country I are brainstorming how to control poverty, create more job opportunities through business model innovation and countermeasures against environmental pollution. The points of discussion are as follows :

Is poverty really the outcome of luxurious passion and fashion of the economists and public policy makers globally today?

Is it rational to copy the concept of chemical equilibrium into economic equilibrium to maintain the stability of the global economy?

Should the government of country I be indifferent to regulate intrusion, migration and infiltration of the refugees from neighbors (e.g. B, P, N) to control poverty and unemployment being provoked by the wise sayings like tolerance, unity in diversity, collaborative intelligence, humanity, actions against promotion of hate crimes and vote bank politics? What are the risks and countermeasures to avoid economic stress in job market and optimal fair resource distribution in country I today? Is it not essential to adopt a strict immigration policy, citizen amendment bill (CAB), national registry of citizens (NRC) and ERP system to curb the problem of intrusion and poverty?

If more resources are allocated and distributed to the poor people of the society by Govt. of I, there will be more intrusion and infiltration from the neighbors to country I and there will be spiraling effects in poverty statistics. The poor people from the neighboring countries will be attracted to the facilities and opportunities adopted by Govt. of country I. The local people of country I are facing the stress in job market and deprived of fair resource allocation and distribution due to the pressure from the refugees / migrants / infiltrators. A large portion of the resources (e.g. space, land, food, energy, utilities) are captured by the refugees, infiltrators and migrants who are involved in setting up their local colony and culture through strategic alliance. Look at the local people of state W of country I. They are forced to migrate to the other states of country I but ill-treated and forced to come back to W. The recent killing of several laborers in state K of country may be a good example of the problem. The migrants are coming to W. They are setting up their own colony, culture and educational system and running parallel government. The migrants and refugees are involved in bad culture ('apasanskriti') and malicious antisocial activities silently through fake broadcast and false data injection attack; the real contributions are big zero; hate crimes (jatibiddesh) are getting originated through a natural process. The resources are getting consumed by the intruders / migrants / refugees in unregulated manner which will surely create problems of resource planning, allocation and distribution in future. It is the time to think scientifically. The local people of I and state W are at war, helpless, victimized and burdened.

So what should be the solution for the burden of intruders/ infiltrators / migrants for poverty control? The conflict between ERP (Enterprise Resource Planning) and emotional economics is inevitable. An interesting solution may be 'Uniform growth and development for all' through collaboration in neighboring countries and proper rehabilitation of the refugees, intruders and infiltrators in the neighboring country /

state through back-propagation mechanism. If more resources are distributed to all the poor people of all neighboring countries (e.g. minimum income) and there is uniform economic development, there will be less intrusion of the refugees towards country I and state W. It may be then easier to tackle the rising problem of poverty and unemployment. Border security force of country I may not be able to tackle the problem of migration and infiltration alone. Country I should help the neighbors following the policy of collaborative intelligence in various domains such as technology management, public policy for poverty control measures and infrastructure development. The ministry of defense, home, foreign and economic affairs of country I are expected to work with governments of neighboring countries closely and jointly. It is a critical issue of fairness, correctness, transparency, accountability and rationality in enterprise resource planning and supply chain management; it is rational to think from the resource based view of a nation, country and state.

The ministers of the aforesaid ministries are also considering several other issues:

- Is the broadcast communication system in country I (e.g. newspapers, TV, radio channels) captured and compromised by the intruders, infiltrators, migrants and refugees from the neighbors?

- Is it rational to focus on traditional old models of Economics for poverty control?

- Are the books on poor economics during hard time really written by the great economists or the same are the outcome of the perception based nonfactual readymade immatured confused thoughts of the students / academic community at the college canteens of the academic institutes? Are all data mentioned in the books on poor economics in hard times authentic or readymade?

Is the resource based view of a firm similar to the resource based view of a nation / state / country? What are the negative impacts of unregulated resource consumption by the intruders, refugees, infiltrators and migrants in a country or a state ? Will not there be shortage of resources in future in country I? If there is unlimited increase in consumption by the intruders and refugees; there may be increase in demand for a firm in short run but there will be shortage of resources and economic stress in job market for the local people of a country in long run! The local folks may be forced to struggle for existence. Did the great economists think from the perspective of optimal enterprise resource planning (ERP) and supply chain management (SCM) in their old time? Does country I need critical thinking and deep analytics on HR and business model innovation today; the problem of poverty is not so trivial at all; traditional old models may be dead and obsolete in modern times! An apparently popular solution may be a disaster due to biased, perception based nonfactual readymade immature confused thoughts of the so called intellectuals! It is a question of the security of a country : be it social security or defense. The ministries have decided to focus on technology management i.e. proper innovation, adoption and diffusion of a set of path breaking technologies to fight against poverty, environmental pollution and creating new job opportunities through business model innovation.

SESSION 2: TECHNOLOGIES for SECURITY AGAINST NATURAL DISASTERS – ARTIFICIAL RAINFALL, ASTRONOMICAL HAZARDS, EARTHQUAKE, BUSH FIRE & EPIDEMIC CONTROL

***Event* : Technology for humanity and global security summit**
***Venue*: Natural disaster security hall, Technology park : Sanada**
***Time* Schedule : 2p.m. - 6p.m., 15.8.2020**
***Agents* : Representatives of various global organizations Technology management experts from science and technology forums, Earth science experts, environmental engineers, scientists.**
Topic of discussion and key focus areas: Natural disaster, artificial rainfall, cloud physics, astronomical hazards, epidemic and pandemic control, bushfire.
Keynote speakers : Prof. Nick Jones, Prof. Gramy Woods, Prof. Bob Roy, Mr. Hansie Rabada, Dr. Kalin Croft, Dr. Hariharan, Mr. Lin, Dr. Han

1. SCOPE

Scope Analytics

***Agents*: Earth scientists, engineers;**
***Moves* : Requirements management, threat analytics;**
***Disasters*: call threat analytics –> assess threats (drought, flood, heavy rainfall, snowfall, storm, sand storm, cyclone, earthquake, volcano, bushfire, woodfire, epidemic, pandemic, astronomical hazards, environmental pollution (air, water, soil, sound, sunlight), (attacks of wild beasts and pastes);**

Prof. Nick Jones and Mr. Lin are exploring the scope of emerging technologies against natural disaster. *Natural disaster* is a critical causal factor of poverty of human society globally. Can emerging technologies be used to fight against natural calamities effectively? How can we assess and mitigate risks of various types of natural disaster such as flood, drught, storm, earthquake, volcano, woodfire, snowfall, epidemic and pandemic outbreak, astronomical hazards, environmental pollution and attack of malicious pastes and wild animals effectively?
Can You recall the tune of 'The rain must fall' by Yanni? This session is analyzing the technological innovation associated with the problem of water security through artificial rainfall and rational, fair and correct resource allocation and sharing among multiple entities. Such type of technological innovation is essential to fight against natural calamities such as drought and flood. It is an emerging technology for humanity. We have analyzed the technological innovation through seven elements of the deep analytics i.e. scope, system, structure, security, strategy, staff-resources and skill-style support of the deep analytics. We have shown various strategic moves of artificial rainfall such as weather modification and rain enhancement through cloud seeding, glaciogenic seeding, hygroscopic seeding and laser induced rainfall. At present, the technology is at emergence phase of

technological life-cycle. We have shown SWOT analysis on various methods of artificial rainfall. This work also outlines a water sharing mechanism (WSM) based on collaborative intelligence. However, the efficiency of the resource sharing mechanism is associated with several critical success factors such as good governance, corporate social responsibilities, law and order, rational positive thinking and political goodwill. An intelligent broadcast protocol is expected to enhance public awareness of rational usage of water by the common people and restrict wastage of water in swimming pools, water amusement parks, luxurious use of air conditioners and air coolers by the rich and super rich classes of our society; tap at roadside and construction works and leakage from pipelines, saving water bodies and conservation of water. Academic institutes and government are expected to play responsible and rational role in regional urban and rural development planning globally. Finally, this work outlines the innovation, diffusion and adoption on emerging laser induced artificial rainfall technology, very large scale integrated smart water grid and water sharing mechanisms based on collaborative planning, forecasting and replenishment.

The expert panel are considering the problem of water security. The people in today's world are facing with significant challenges in this utility sector such as shortage of water, high cost of generation, storage and distribution, wastage or loss and pollution. We must set an efficient national and global utility policy to promote the development of a sustainable system which should be viable environmentally, socially and economically. The sustainability in such resource management not only requires a balanced approach between natural and artificial rainfall but also encourages rational and efficient use of water by minimizing wastage and pollution. There are many strategic moves of efficient water resource management. This work is focused on two specific strategic moves to fight against flood and drought: artificial rainfall and multi-agent collaborative resource sharing. Can we dream of a collaborative enterprise model in this context?

This session is also also exploring the problem of private search and presents three private search algorithms for three test cases – (a) real-time moving target search to detect astronomical hazards; (b) Real time private moving target search for robot navigation and (c) Private Light Beam Search. The basic objective of a search is to identify an object and the position of the target. The target's position may be uncertain or there may be complete or incomplete information about its location in terms of a probability distribution. The target may be stationary or in motion. The target distribution is associated with discrete or continuous search space. The problem of optimal search is to maximize the probability of detecting a target subject to the constraints of resources, effort and time. Adaptive security and dynamic data management (DDM) is an essential part of space technology that can monitor the space in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. This session also presents Real-time Probabilistic Search Mechanism (RPSM). The probabilistic search approach addresses the incomplete information on the target location by location probability. The problem is probabilistic from the perspectives of the location, size, distance and timing of the

moving target(s) and distribution of the search efforts. The effectiveness of probabilistic search procedure can be verified on the basis of various properties of adaptive secure multiparty computation such as correctness, privacy, transparency, reliability and consistency. The search space can be divided into a set of private blocks; adequate number of sensors should be assigned to each private block; each block is monitored independently. This work highlights the complexity analysis of RPSM from the perspectives of computational cost and security intelligence. It also exercises case based reasoning on a test case of astronomical hazards and explores the scope of RPSM to assess and mitigate those threats. The universe is basically a computer, its history is being computed continuously. The astronomical hazards may be really dangerous threats against the sustainability of today's human civilization and the existence of a safe earth. This type of probabilistic search problem is really hard to solve, it is not a trivial problem. It is also challenging to deploy automated real-time search in reality and seeks extensive support, coordination, planning and corporate social responsibilities from various space research organizations and earth science institutes globally. Today, we have been dreaming of the moon and Mars voyage in space research. It may be a hard target. But, the sustainability of our earth from the dangerous astronomical hazards should be a top priority in space research globally: isn't it rational?

The basic objective of a search is to identify an object and the position of the target. The target's position may be uncertain or there may be complete or incomplete information about its location in terms of a probability distribution. The target may be stationary or in motion. The target distribution is associated with discrete or continuous search space. Search is conducted with various types of sensors such as CCTVs, cameras, telescopes, satellites and eyes of human agents. A detection function gives the probability of detection for a search as a function of effort (e.g. swept area, time). The detection function evaluates the effectiveness of search efforts in terms of probability of detecting the target object. The problem of optimal search is to maximize the probability of detecting a target subject to the constraints of resources, effort and time. The search space can be divided into a set of private blocks; adequate number of resources (sensors) can be assigned to each private block; each block is monitored independently.

In a search problem, a searching agent tries to find a hidden object by screening a certain defined area. The search space may be either discrete or continuous. In a continuous space, the target may move in various ways such as random, Markovian or Brownian moves. If the location of the target is known, then it may be complete-information tractable search problem and it may detect the target with a minimal number of search moves. The exact location of the target is generally unknown to the searching agent in incomplete information search and the problem is addressed using the concepts of fuzzy logic or probability theory. The probabilistic search approach addresses the incomplete information on the target location by location probability. The problem is probabilistic from the perspectives of the location of the target and distribution of the search efforts. The effectiveness of probabilistic search procedure can be verified on the basis of various properties of secure multiparty computation: correctness (i.e. correct identification of the targets), privacy, transparency, reliability and consistency.

The problem of optimal search for a moving target in both discrete and continuous space has been investigated extensively in various research articles on operations research and artificial intelligence. This work is an attempt to extend the study on the basis of related literature review and case based reasoning. This work is organized as follows. Section 1 is focused on scope; it defines the problem of probabilistic search of moving targets in discrete and continuous space.

This session also explores the scope of other natural disasters including epidemic and pandemic outbreak and bushfire and suggests a set of intelligent strategic moves as countermeasures. It is rational to adopt an efficient system; an optimal mix of e-governance (e.g. online grievance management system), broadcast communication protocol and artificial immune mechansism to fight against natural disaster, epidemic and pandemic outbreak. There is threat of bio-terrorism on the soft targets (e.g. life-science supply chain and healthcare service chain). Is the conflict between security intelligence and business intelligence inevitable? It is an interesting observations that technologies for humanity can be effectively applied to fight against disasters. *Pandemic* is more dangerous than *epidemic*. When an epidemic spreads globally, it is called pandemic. In case of epidemic, a disease spreads at very fast rate witin a particular period among one or more communities. For example, WHO has recently declared the outbreak of novel Corona virus as Pandemic, but it is controllable. There are other various types of threats of epidemic globally due to environmental pollution such as air, water, soil, light and sound pollution.

a) Epidemic due to *air pollution* like dust at construction sites and industrial plants; smoke from vehicles; paste control problem (e.g. mosquitoes, flies), malnutrition in slum areas, improper cleaning of garbages and stool of street animals?

b) Epidemic due to *water pollution* in supply of dirty drinking tap water caused by leakage in pipelines, contamination and jerms in water storage system, malfunctioning of tube wells, water filtering problem, mixing of water from drainage system and tap water pipeline, unprotected selling of unhealthy food (e.g. oily spicy biriyani) and beverages at retail outlets and by hawkers being contaminated by flies; risks of diahorrea, stomach upset and loose motion.

c) Epidemic due to *soil pollution* and earthquake caused by random digging of soil for construction projects, erosion of soil at riverbeds; jamming in drains due to plastics, improper cleaning of drainage and sewage system;

d) Epidemic due to *light pollution* in slum areas, unplanned urban development planning, blockage of sufficient sunlight into residential areas (e.g. houses, flats, multi-storied buildings)

e) Epidemic due to *sound pollution* caused by playing loud and wild music, fireworks, activities at construction sites and industrial belts.

The key focus areas of this session are artificial rainfall, cloud seeding, collaborative intelligence, resource sharing mechanism, water sharing, compensation, collaborative planning, forecasting & replenishment, political will, power play, conspiracy for war, corporate social responsibilities, artificial intelligence, probabilistic light beam search, predictive threat analytics, astronomical hazards, reactive and proactive security, private search, adaptive security, dynamic data management, natural disaster, epidemic control, pandemic

outbreak, intelligent broadcast, online grievance management system, articial immune mechanism, self-Nonself classification, danger signal, clonal selection, hotspot, cluster, social distancing, security intelligence, business intelligence, bio-terrorism, life science supply chain and healthcare service chain.

2. SYSTEM

System Analytics
***Agents*: Earth scientists, environmental engineers;**
***Moves* : requirements engineering, system design, prototype testing, erection, installation, testing, commissioning;**
***Emerging technologies*: innovate a set of emerging technologies based on threats.**

- ✪ **Drought and heatwave : Earth science – artificial rainfall, cloud seeding using laser technology and cloud physics; civil – water storage system, irrigation system ; mechanical – air conditioining system, air coolers, water pipeline; electrical – solar water pumps; logistics engineering – rail, ship, truck;**
- ✪ **Flood / heavy rainfall : Earth science – cloud diversion; civil – dams, water conservation system, storage, drainage and irrigation system; mechanical – boats, helicopters, drones, planes; electrical – motors and pumps;**
- ✪ **Snowfall : mechanical – excavators, ice breakers; electrical – room heaters;**
- ✪ **Storm / cyclone / sandstorm : Earth science - predictive analytics; civil – robust housing structure; mechanical - excavator, electrical - fault analytics, power cut, standalone roof top solar panel;**
- ✪ **Earthquake : Earth science – predictive analytics, geographical information system ; civil - earthquake proof light weight, flexible housing structure; mechanical and metallurgical – steel, aluminium, glass; electrical – protection from open circuit, short circuit, transients and power cut;**
- ✪ **Volcano : Earth science – predictive analytics; logistics system – evacuation system, rail cars, bus, trucks, planes, helicopters; civil : safety chambers;**
- ✪ **Bushfire : mechanical – water piepine, electrical – solar water pumps, lightning arrester; chemical – smoke, fire extinguishing system;**
- ✪ **Epidemic / pandemic: Pharmaceutical engineering – vaccines, precision medicines, healthcare engineering, biotechnology engineering;**
- ✪ **Astronomical hazards : Earth science and digital technology - predictive analytics, real-time moving target search, satellite communication; civil – safety shelter, cave, robust housing structure; mechanical – strong, reliable materials; electrical - fault analytics; chemical – fire extinguishing system;**
- ✪ **Environmental pollution : environmental engineering (air, water, soil, sound, sunlight); civil – soil erosion control, restriction on soil digging, drainage system, nano housing architecture; mechanical – smoke emission control from vehicles, waste treatment plants;**
- ✪ **Attacks of wild beasts and pastes : conservation of forests; civil - wall; mechsanical, rubber bullet, electrical - fence; chemical - gas bombs; digital / electronics – music system;**

Prof. Bob Roy and Dr. Hariharan are discussing on the system associated with emerging technologies against various types of natural disaster, Natural rainfall requires conservation of forests and green plantation in smart cities and villages and along riverside. It is essential to save the rivers. Massive cut of trees and green plants in urban zone occurs due to construction of residential flats and other civil infrastructure (e.g. flyovers, bridges and transportation infrastructure). It may lead to droughts. The basic objectives of rainmaking or artificial precipitation or artificial rainfall is to artificially induce or increase precipitation using airplanes or rockets to sow to the clouds with catalysts. This method makes rain or increase precipitation and drought like situation.

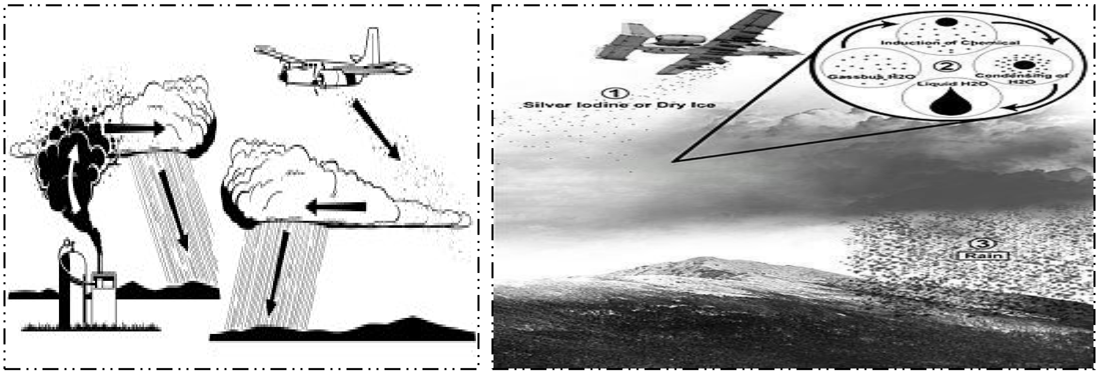


Figure 2.1: Cloud Seeding

Cloud seeding is a weather modification method by dispersing substances into the air ; results condensation of cloud and alter the microphysical processes within the cloud [6-10]. The most common chemicals used for cloud seeding are salt powder (e.g. silver iodide, potassium iodide), dry ice and liquid propane. Cloud seeding chemicals may be dispersed by aircraft or drones or by dispersion devices located on the ground (e.g. firing from anti-aircraft guns or rockets) (Figure 2.1).
Glaciogenic cloud seeding use glaciogenic materials such as Silver Iodide which increase the ice crystal concentration in clouds by freezing cloud droplets. Static cloud seeding is applicable to cold cloud. Dynamic seeding results increased rainfall as compared to the static approach. The seeding of super cooled cloud with large amount of ice nuclei cause glaciation of the cloud. The super cooled liquid water is converted into ice flakes releasing latent heat, increasing buoyancy, growing larger and increased precipitation. Hygroscopic cloud seeding is a form of warm cloud seeding which enhances rainfall through coalescence process using fine spray of hygroscopic salt.
The other emerging techniques for artificial rainfall are laser induced cloud generation and ion generation method. Lasers may help causing rain; rainclouds form when airborne pockets of tiny particles condense water vapor around them (Figure 2.2). It is possible to control over moisture using laser. Weather control may get their next rainmaking tool in the form of an infrared laser. Precipitation is formed after lightning and heavy rain follows due to dissociation, ionization and natural seeding process in the atmosphere. Plasma laser pulse can be used for artificial rain making; for example 2.2 x 10^{19} gm of water drops are formed in the

atmosphere by laser pulse of energy 500 mJ. Plasma laser pulse creates high temperature (up to 3000^{o}C) which breaks bonds N_2 and O_2 into excited and unstable N* and O* and form NO and O_3. These endothermic reactions absorb heat from the clouds and condensation creates water drops. Simultaneously N_2 and O_2 will be ionized and become big clustered ions through several

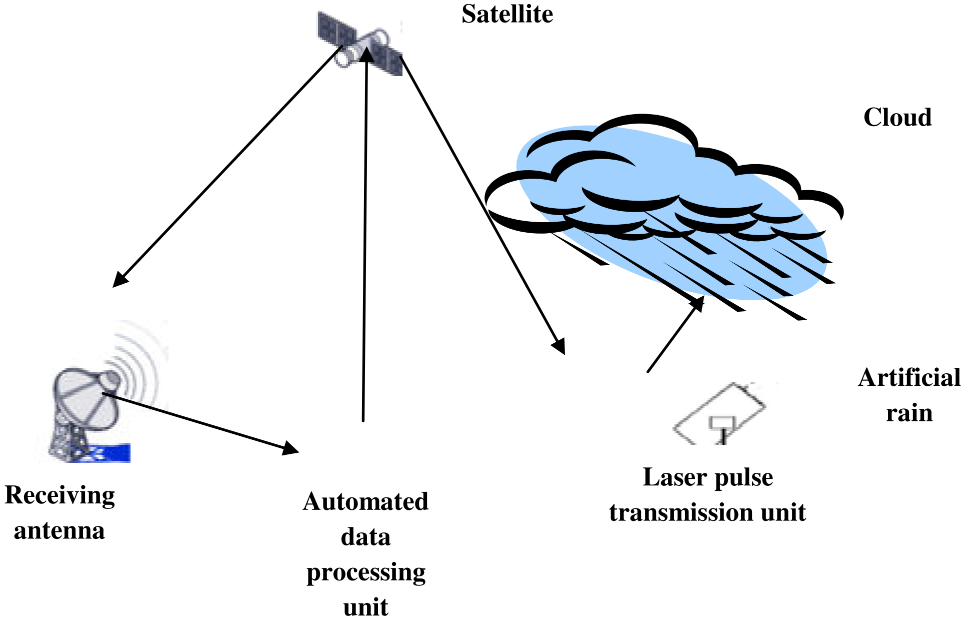


Figure 2.2 : Laser induced artificial rain

reaction. The big ions act as seed and results precipitation and rain.

Self-guided filaments generated by ultra short laser pulses is an emerging technology to assist water condensation, in an under saturated free atmosphere based on photo-oxidative chemistry and electrostatic effects. The phenomenon is used for remote characterization of humid atmosphere, triggering of water precipitation and cloud formation. Laser based condensation is a remote sensing nucleation processes in clouds influencing or triggering water precipitation. Self-guided laser filaments result from a nonlinear propagation regime of ultra-short laser pulses. Beyond a critical power (P_{cr} = 3 GW in air at a wavelength of 800 nm), the beam self-focuses due to the optical Kerr effect until its intensity is sufficient to allow multi-photon ionization of air molecules generating a cold plasma. At this point, the released free electrons (typically 10^{15}–10^{16} cm) and the negative higher-order Kerr terms tend to defocus the beam and dynamically balance Kerr self-focusing. one or several self-guided filaments with a diameter of 100 μm are generated over distances much longer than the Rayleigh length, up to hundreds of meters. Filaments can be initiated at predefined remote distances and propagate through adverse conditions including fog and clouds, turbulence or reduced pressures.

Test case : Private real-time moving target search for astronomical hazards

Real-Time Probabilistic Search Mechanism (RPSM)

Input:* s*earch space, goal state, target distribution, detection function;

Output: **Identify objects (e.g. moving targets);**
Critical parameters : Target goal state, search space, detection function
Moves:

- **Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities;**
- **Real-time search;**
- **Automated data stream mining by intelligent threat analytics,**
- **Adaptive secure multi-party computation**
    - **Access control: audit authentication, authorization and correct identification, privacy;**
    - **Secure computation: verify correctness, fairness, rationality, trust, commitment, transparency, accountability;**
    - **System verification: verify safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**

Procedure (Probabilistic Search):

Divide the search space into a set of private blocks;
Assign resources to each private block;
Project light beam on private search space → move forward and backward;
Search discrete or continuous search space → sense data stream → filter data stream;
Detect target → verify correctness → give alert.

Security measures : **(a) Proactive (b) Reactive.**

The aforesaid mechanism (RPSM) is defined by a set of elements: system, searching agents, a finite set of inputs, a finite set of outcomes as defined by output function, a set of objective functions and constraints, an optimal set of moves, revelation principle, security measures and search procedure. It evaluates a system which is defined by a set of states (e.g. initial, goal, local and global) and state transition relations. The mechanism seeks the support of an intelligent reasoning system i.e. threat analytics.

Private Light Beam Search Algorithm : Let us analyze the aforesaid private search algorithm which is basically an interactive search. The cost of computation of probabilistic search depends on light beam projection on private search space. Let us show an illustration of private search. The basic steps of an interactive search algorithm which operates between a decision making agent (DMA) and the mediator agent (MA) are as follows: (a) MA computes an initial feasible solution. (b) MA interacts with the DMA and (c) MA obtains a (or a set of) new solution. If the new solution or one of the previous solutions is acceptable to the DMA, stop. Otherwise, go to step 2. The design of interactive search methods depends on various issues: (a) The form through which DMA gives information, (b) The approach by which a multi-objective problem is transformed into a single objective problem, (c) The type of data used for interaction with DMA, (d) Number of non-dominated points to be presented to the DMA (a single point or a sample of points) and (e) How the DMA evaluates a set of alternatives?

Agents **: A decision-making agent (DMA) and the mediator agent (MA).**
Input **: The mediator holds the deterministic problem; The DMA holds its aspiration point, reservation point, indifferent threshold, strong and weak preference threshold and veto threshold.**
Output**: DMA knows a set of solutions; MA can not know the output.**
1. MA requests the DMA to specify its preferential parameters (P_A,P_R,I_{th}, P_{th}, S_{th}, W_{th}, V_{th}).
2.The DMA generates (n-1) random set of preferential parameters and appends its desired set of preferential parameters at a random position. The DMA sends to MA the list H = (H_1,…,H_n) where for a secret index $1 \leq j \leq n$, H_j = (P_A, P_R, I_{th}, P_{th}, S_{th}, W_{th}, V_{th}).
3. Repeat until the DMA is satisfied with a solution or concludes that no compromise point exists for the present constraints
a. MA computes a middle point (MP) alongwith characteristic neighbors for each set of preferential parameters.
b. The DMA gets back the results of k middle points alongwith characteristic neighbors using k-out-of-n oblivious transfer protocol where k<<n.; DMA scans the inner area of the current neighborhood and stores its preferred solutions in a private list L_1; it stores the invalid middle points in a private list L_2.
c. Case
1. The DMA wants to define a new aspiration and/or reservation point and/or updates preferential thresholds:

- **The DMA adds a set of new aspiration and/or reservation points and/or new preferential thresholds to the list H and sends H to MA.**
- **MA projects the aspiration points onto the non-dominated set and generates middle points**
  with characteristic neighborhood.
- **The DMA gets back the result of desired middle point alongwith characteristics neighbors**
  using 1-out-of-n oblivious transfer protocol.

2. ***The DMA wants a point from the current neighborhood to be the new middle point or wants to return to one of the stored points of L_1:***

- **The DMA adds the desired middle point to the list L_2 and sends L_2 to MA;**
- **MA generates neighborhood of the middle points.**
- **The DMA gets back the result of desired middle point alongwith characteristics neighbors using 1-out-of-n oblivious transfer protocol.**

Let us consider a specific interactive search procedure called *Light Beam Search* (LBS) method The idea of light beam search is analogous to projecting a focused beam of light from the aspiration point onto the search space [Figure 2.3]. The lighted part of the frontier changes if the *aspiration point* or the point of interest in the non-dominated set is changed. This interactive search occurs between a DMA and the MA. The mediator asks the DMA to specify its preference in the form of aspiration and reservation point and various types of preferential thresholds. At each iteration of LBS procedure, MA generates a sample of non-dominated points

using this preferential information. The sample is composed of a middle point and a set of non-dominated points from its neighborhood. MA shows these points to the decision-making agent.

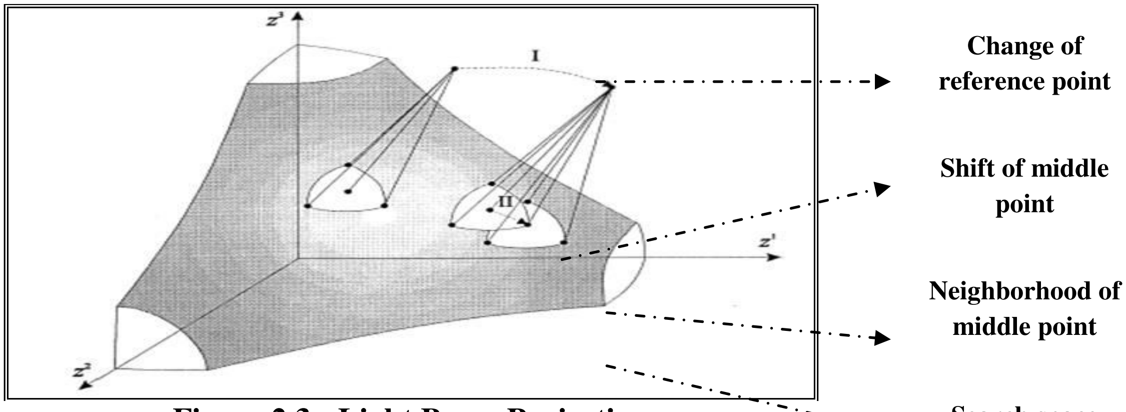


Figure 2.3 : Light Beam Projection

Private light beam search preserves the privacy of individual preferential parameters of the decision making agents about the target goal in terms of aspiration point (P_A), reservation point (P_R), indifferent threshold (I_{th}), strong preference threshold (S_{th}), weak preference threshold (W_{th}), veto threshold (V_{th}), middle point (MP) and preferred solutions resulted from the search process. The mediator agent preserves the privacy of the search problem. The value of an objective function which is desirable or satisfactory to the decision maker is called *aspiration point*. The value of an objective function that the decision maker wants to avoid is called *reservation point*. A decision vector $x^* \in S$ is pareto optimal if there does not exist another decision vector $x \in S$ such that $f_i(x) \leq f_i(x^*)$ for all i =1,…,k and $f_j(x) < f_j(x^*)$ for at least one index j; f_i is objective function and S is feasible space. An objective vector $z^* \in Z$ is pareto optimal if there does not exist another objective vector $z \in Z$ such that $z_i \leq z_i^*$ for all i =1,…,k and $z_j < z_j^*$ for at least one index j.

The decision maker should inform the mediator various *preference thresholds* in order to compare alternatives and to define outranking relations. There is an interval of preference wherein it is not possible for the decision-making agent to distinguish between different alternatives due to imprecision and uncertainty of measurements and this corresponds to *indifference threshold*. *Strict preference threshold* is defined as minimal increase/decrease of any objective that makes the new alternative strictly preferred with respect to this objective. There exists an intermediate region between indifference and strict preference threshold where the decision-making agent hesitates to compare alternatives. This corresponds to *weak preference threshold*. *Veto threshold* It indicates that what is the minimal increase/decrease of any objective that makes the new alternative unacceptable regardless of the value of other objectives. In each computation phase of search, a finite sample of non-dominated points is generated by the mediator agent. The sample is composed of a middle point and a set of points within its *neighborhood*. The starting middle point is obtained by projecting aspiration point on the non-dominated set in the direction of reservation point. For a middle point, the

neighborhood is defined as a set of non-dominated points that are not worse than the middle point. The neighborhood points from the sample indicate to what extent the values of particular objectives can be improved in relation to the *middle point*.

Test case : Private real-time moving target search algorithm for robotic navigation

The goal state of private search algorithm may be fixed or may change during the course of search. The goal may be a target which actively avoids the searching agent or object. In case of robot navigation In a moving target search algorithm, if the average speed of target robot is slower than that of the problem solving search agent, the later is guaranteed to eventually reach the target in a connected problem space. The algorithm is expected to be efficient in terms of minimum operations necessary to guarantee its completeness, commitment to reach the target goal and deliberation for selecting plan as per the principle of resource based planning. The target robot may be reaching the problem solving robot cooperatively or avoiding the same. The target robot may not stop eventually. The goal is achieved when the position of the problem solving robot and target robot coincide. If the problem solving robot moves faster than the target robot, the goal may be achieved. Otherwise, the target robot could evade the problem solving robot infinitely even in a finite problem solving space by avoiding in a dead end path.

Private Real-time Moving Target Search Mechanism
Agents / Objects : Problem solving agent(s), Target agent(s);
Scope :

- **Goal / Changing goal of moving target(s)**
- **Constraints : Space complexity, Time complexity, uncertainty in movement of target(s);**

System :

- ✓ **Input: x – current position of search agent; y – current position of target; z – current speed of search agent;**
- ✓ **Output : Adaptive search plan;**
- ✓ **Procedure**
    - ▪ **Case 1 : When problem solving search agent moves**
        - **Calculate h(x',y) for each neighbor x' of x;**
        - **Update the value of h(x,y); $h(x,y) \leftarrow \max (h(x,y), \min_{x'}[h(x'y)+1]$;**
        - **Move to the neighbor x' with minimum h(x',y); assign the value of x' to x; ties are broken randomly.**
    - ▪ **Case 2 : When the target agent moves**
        - **Calculate h(x,y') for new position y' of target;**
        - **Update the value of h(x,y) : $h(x,y) \leftarrow \max [h(x,y), \{h(x, y') - 1\}]$;**
        - **Set the new goal of the searching agent as the new position of the target; assign the value of y' to y.**

Structure : The search space consists of a set of nodes connected through edges.
Security : Verify security intelligence of searching mechanism,

- **Access control : A or a set of authorized problem solving search agent(s) should be able to communicate and exchange data through authenticated channel and correctly identify target agent(s) in time.**
- **Privacy in revelation principle: The problem solving agent(s) hide own speed and position from the target(s).**
- **Audit rationality, commitment of trust of searching agents.**
- **Verify fairness and correctness of heuristics estimate of distance, speed and position of the targets).**
- **Asses the risks of corruption of searching agent(s) (e.g. problem solving robot).**
- **Verify reliability, consistency, deadlock-freeness, reachability and resiliency of the search process.**
- **Assess the risks of malicious attacks: Denial of service, false data injection and Sybil attack.**

Strategy : Adaptive real-time private moving target search – depth first search, breadth first search or a combination of the two;
Resources : Allocate adequate resources for search and private communication.
Skill-style-support: Ensure transparency, accountability, collaboration, coordination and and resource based planning in private search.

***Analysis of Private Search Algorithm* : The efficiency of private moving target search is evaluated n terms of space complexity and time complexity. The upper bound on the space complexity of private moving target search is n^2 where n is the number of states in the problem space. The overall space complexity is the minimum of n^2 and the total number of moves of the problem solving search agent and target. The worst-case time complexity of private search is n^3 where n is the number of states in the problem space. It can be obtained based on maximum heuristic disparity. The total heuristic error is upper bounded by n^3 and the maximum heuristic value of each state is n. If no updates of heuristic values occur, the maximum number of moves of the problem solver to reach the target is n = w where w is fraction of moves skipped by the target. Over the course of a single problem solving episode, the searching agent gradually learns more accurate heuristic values until the target is reached. Next issue is the speed of the search agent and the target. There are two possibilities. The search agent can move faster than the target but it is not strictly necessary. A weaker condition is that the target may move as fast as the search agent, but occasionally makes errors in avoiding the problem solver. Finally, the complexity of private search depends on available information about the target by the search agent. Is it really valid that the search agent always knows the position of the target. The search agent must try to know the position of the target at some point before it reaches the last known position of the target.**
The basic building block of private search algorithms is *adaptive secure multi-party computation.* Let us first discuss the traditional concept of secure multi-party computation. Two or more agents want to conduct a computation based on their private inputs but neither of them wants to share its proprietary data set to other. The objective of secure multiparty computation (SMC) is to compute with each

party's private input such that in the end only the output is known and the private inputs are not disclosed except those which can be logically or mathematically derived from the output. In case of secure multi-party computation, a single building block may not be sufficient to do a task; a series of steps should be executed to solve the given problem. Such a well-defined series of steps is called a SMC protocol.

In the study of SMC problems, two models are commonly assumed: semi-honest model and malicious model. A semi-honest party follows the protocol properly with correct input. But after the execution of the protocol, it is free to use all its intermediate computations to compromise privacy. A malicious party does not need to follow the protocol properly with correct input; it can enter the protocol with an incorrect input. Adaptive secure multi-party computation deals with adaptive adversaries that may choose the corrupted parties during the course of computation in a setting of insecure communication channels. In case of Non-adaptive secure multi-party computation, the set of corrupted parties is arbitrary but fixed before the computation starts.

A search protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. Secure multi-party computation preserves privacy of data in different ways such as adding random noise to data, splitting a message into multiple parts randomly and sending each part to a DMA through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. Security and privacy of critical data is an important concern in any search procedure. Existing literature on private search is highly focused on the construction of various types of cryptographic tools (e.g. encryption and decryption, signcryption) and query processing on encrypted data as per the needs of revelation principle, information disclosure and privacy policy and risks of corruption of a mechanism. But it is not the only serious concern in a probabilistic search procedure. Let us define the private search on the basis of adaptive secure multi-party computation from a new outlook.

The security intelligence of the private probabilistic search procedure is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy. The search procedure addresses the issues of authentication, authorization, correct identification, privacy and audit through cryptographic solutions. For private search, the system should ask the identity and *authentication* of one or more agents involved in the mechanism. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After the identification and authentication, the procedure should address the issue of *authorization*. The system should be configured in such a way that an unauthorized agent cannot perform any

searching task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. *Privacy* is another important issue; a searching agent can view only the information according to authorized access rights. The search procedure preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication. Privacy is the primary concern of the revelation principle of a private search; the issue can be addressed through the concept of cryptography to provide confidentiality, data integrity, authentication and non-repudiation.

Traditionally, cryptographic solutions are focused to ensure information security and privacy. But there are other different types of cryptographic concerns since the security intelligence is evaluated in terms of fairness, correctness, transparency, accountability, confidentiality and trust. The search mechanism is expected to ensures *correctness* in correct detection of target objects through adaptive real-time data mining and secure communication among the searching agents free from any false data injection attack; each recipient must receive the same correct data in time without any change and modification done by any malicious agent. *Fairness* is associated with the commitment, honesty and rational reasoning and trust. Fairness ensures that something will or will not occur infinitely often under certain conditions; it is important from the perspective of fair resource allocation in a search procedure. The search procedure must ensure the *accountability* and responsibility of the searching agents in access control and data mining. In fact, accountability is associated with collective intelligence. The *transparency* of the procedure is associated with communication protocols, revelation principle and automated system verification procedures (e.g. group testing). For example, a procedure should clearly state its goal state.

The performance and quality of search is expected to be consistent and reliable; it should be validated through *audit* of probabilistic search procedure. *Reachability* ensures that some particular state or situation can be reached. *Safety* indicates that under certain conditions, an event never occurs. *Liveness* ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. The effectiveness of probabilistic search procedure is expected to be verified adaptively on the basis of correctness, privacy, transparency, reliability and consistency. *Adaptability* is about responding to change effectively and decisively through real-time search: the ability to identify the change in search space for the moving targets, understanding the probable impacts of the hit by the targets, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation. The aforesaid discussion gives a complete definition of 'private search' based on adaptive secure multiparty-computation.

4. STRUCTURE

Structure Analytics

***Agents*: System analysts, business analysts;**
***Moves*: Design and configure**

- **Organization structure : Technology forums; National level : Government, NGOs, research organizations; International level : strategic alliance among global organizations;**
- **System architecture ; Innovate a set of emerging technologies;**
    - ***Level 1*: earth science, information technology, electrical, electronics, chemical, mechanical, civil, biotechnology, pharmaceutical engineering;**
    - ***Level 2*:**
        - ***Earth Science***
            - **Receiving antenna, satellite, laser pulse transmission unit, automated data processing unit; / * for artificial rainfall) */**
            - **Astromonical hazards : telescopes, search agents, sensors,;**
        - ***Information technology* :**
            - **Define computing, data, networking, security and application schema of artificial immune system, e-governance, real-time data tracking system.**

Mr. Lin and Dr. S. Chakraborty are giving the basic overview of the structure on emerging technologies against natural disaster. The laser induced artificial rainfall system consists of a receiver unit, processor unit and transmission unit. These components communicate with each other through satellites. The receiver unit receives the data about the clouds (e.g. temperature, humidity, height from earth surface, pressure) and the data of demand of rain for a zone. The processor unit processes the transmitted data, computes the intensity and pulse duration of plasma laser and selects the right transmission unit to trigger laser induced artificial rainfall. A particular zone may be assigned to more than one transmission units as per demand. The transmission unit sends a laser pulse in the given direction of the intensity computed by the processor. This unit is connected to processor unit through satellites. More than none transmission units may be connected to a centrally located receiver and processor unit. It cuts cost of the laser induced rainfall system and may cover larger region.

The transmitter could be a terawatt femtosecond Ti sapphire pulse laser; fundamental wavelength may be ~800nm; pulse energy ~400mJ, duration 100fs and repetition frequency of 10-100Hz. The laser pulse propagates with almost high peak intensity over a distance of ~500m. The transmitter unit should be mounted on a moving platform to cover large area as per demand. This nonlinear phenomenon is caused by the subtle interplay between self-focusing induced by optical Kerr effect and the defocusing by the self-generated plasma. It is essential to compute the power

and wavelength of laser for bond breaking and ionization at the cloud height of 500m. The system is controlled by a Micro Controller remote unit having data acquisition and processing system, fast transient digitizer and computer controlled stepper motors. The laser beam energy is adjusted by the stepper motor. The system is operated by a MV power supply. Initially the beam will be of 15 cm arc and the beam expander vary the width of the beam to get significant amount of rain. A movable mirror directs the beam in the larger area of the atmosphere. It is also required to compute the cross-section of the beam for rainfall to cover a reasonably wider area.

The next element of the deep analytics is structure which should be analyzed from the perspective of organization structure and system architecture. The technological innovation related to the artificial rainfall and multi-agent resource sharing mechanism is suitable for a collaborative enterprise model. The system architecture is shown in figure at an abstract level. Let us also consider the structure of an information system to be used in allocation and sharing of water. The information system should monitor a set of entities such as various water bodies, rivers, canals, lakes and dams; demand of water in agriculture, industrial plants and domestic uses, supply of water, rainfall data, water level in rivers, lakes and storage systems, pollution levels and water sharing data (Reference: Table 2.1). It may be integrated with GIS. The information system is expected to support the decision making process associated with artificial rainfall i.e. what initiatives are essential to fulfill the demand-supply gap. The resource sharing system should be able to interact with various types of sensors and measuring instruments like water level indicator, inflow and outflow measuring instruments physically for real-time supply chain optimization in water resource management. The resource sharing mechanism may also require an intelligent negotiation support system (NSS) for multi-party negotiation in water sharing; it is basically a group decision support system; it permits collection of different views of the negotiating agents; defines the structure of the problem, generates alternatives for compromise and improves the quality and the acceptability of a negotiated agreement.

Entities	Demand of water	Supply of water	Rainfall data	Water level	Pollution level	Water sharing
Water bodies	Agriculture	Rainfall	Natural rainfall	Water bodies : rivers, lakes	Pollutants, plastic, paper	Inflow
Canals	Industry	Sharing from other sources	Artificial rainfall	Dams	Drainage system	Outflow
Rivers	Domestic use of population	Capacity utilization		Storag e system	Congestion	Shared data
Lakes	Drinking, cooking	Loss or wastage			Encroachme nt statistics	Surplus

Dams	**Washing and cleaning**					**Shortage**
Lock gates	**Natural activities and bathing**					

Table 2.1: Analytics for resource allocation and sharing

4. SECURITY

Security Analytics

***Organization* : global earth science organizations;**

***Verification mechanism*: audit *security intelligence*.**

- ***security policy*: verify rationality, fairness, correctness, transparency, accountability, trust and commitment;**
- ***system performance:* verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness, reachability, synchronization, safety;**
- ***multi-party corruption:* do surveillance through security council of global organization, police, army, detectives, journalists ;**
    - **Safety *from natural disaster***
    - **Safety from war, bioterrorism and acts of terrorisms**
- ***access control*: verify authentication, authorization, correct identification, privacy, audit confidentiality, data integrity and non-repudiation;**
- ***malicious attacks*: verify the risk of false data injection, denial of service (DoS) and fault injection attack;**

call threat analytics and assess risks of emerging technologies:

- **what is corrupted or compromised (agents, computing schema, communication schema, data schema, application schema)?**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights : how and why did it occur? do cause-effect analysis on performance, sensitivity, trends, exception and alerts.**
- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**

***Output*: security intelligence**

Dr. Kalin Croft and Dr. Han are debating on the security intelligence of emerging technologies against natural disasters. The security of the technological innovation related to artificial rainfall and multi-agent collaborative resource sharing mechanism should be analyzed from the perspectives of fairness, correctness, transparency, accountability, reliability, consistency, resiliency, authorization and authentication in access control, trust and commitment. It is really a hard task to estimate the resource to be allocated and shared fairly and correctly in time. The resource sharing mechanism should be transparent to all the stakeholders through intelligent broadcast communication. The operators and the administrators of the system should be accountable for any mishap due to the natural disaster such as timely release of water from the dam during heavy rainfall in the rainy season or

proper storage of water in the dam during the summer and the winter for proper irrigation to the fields of agriculture. The performance of the system is expected to be evaluated in terms of reliability and consistency. Who will take the decision of artificial rain? The system should be operated by the authenticated and authorized decision making agents only since it is a very sensitive issue, which is related to the safety and security of a large number of human beings, plants and animals over a specific zone (e.g. it may be a district or a state or even a country).

A group of authorized agents should be able to access the technology of artificial rainfall. They should be able to communicate through authenticated channels for taking important decisions on artificial rainfall. They should be able to identify correctly the demand of artificial rainfall based on evaluation of drought and flood in a country. The decisions should be evaluated and justified based on fairness, correctness, transparency of resource sharing policy, accountability of DMA, rationality, trust and commitment. Rationality is the most important decision making factor of artificial rainfall.. There are threats of multi-party corruptions and various types of malicious attacks on the technology of artificial rainfall and cloud seeding technology. The system should be free of denial of service attack, false data injection, Sybil, shilling and fault attack. The system performance should be verified in terms of reliability, consistency, resiliency, liveness, safety, deadlock freeness and reachability. Flaws in rational decision making may result flood or drought in critical zones globally.

Test case : Water Riot

Prof. Hariharan is presenting a case of water sharing conflict between two states U (upstream state) and D (downstream state) associated with a river (R). There is lack of mutual cooperation and trust between two states in the context of water sharing of river R. Initially, the Supreme Court (SC) orders the state government of U to release water of 15000 cusec / day; then 12000 cusec / day; then 6000 cusec water / day to the state D. There was a water riot in state U; the mob torched 42 buses; a leader was killed. Inlow from U was 15000 cusecs/ day last week. 12000 cusecs was being released everyday from Dam X from 20.9.2016. Release amounts to 1 tmcft; paddy raised in 14.9 L acres. Then, the inflow from U was reduced to 3000 cusecs on Wednesday evening; 21.9.2016. SC orders U to release 6000 cusec water / day for rest of September'2016. The State Govt. of U called all party meeting and had taken decision collectively; a legislative resolution was taken to defy SC order; stop release of water for agriculture (e.g. samba cropping) and water to be released only for drinking purpose.

The State Govt. of D did not call any all party meeting. This is a fresh controversy. Defiant U triggers a constitutional crisis since it is defying SC order to release 6000 cusecs per day to TN. The special legislature session is expected to adopt a resolution that SC order cannot be implemented as it is contrary to the public interest in the state U. U does not have adequate drinking water. By projecting it a legislature-judiciary confrontation, the state Govt. of U hopes to escape the charge of commitment to the court.

Many in U are concerned with the silence of the central government. The centre can not be a bystander since the issue is with the Supreme Court (SC). The PM should

take initiatives to prevent a constitutional crisis. It is his duty to protect the federal structure. The decision of the Govt. of U cannot be seen as an act of defiance but as the helplessness of a state ravaged by a court order that cannot be implemented. If U defies SC order, then there are serious risks for river sharing agreements. The tension between U and D will grow since both states are feeling pressure. Outright defiance of SC may boomerang and set an extremely dangerous precedent. SC directs to form river R board having representatives from four neighboring states U,D, Y and Z. Even in the absence of state representative, the board can take decisions by majority option. So, it is in the interest of the riparian states to nominate the members otherwise they will lose the opportunity to protect their rights.

The output of the analytics is as follows: Irrigation in state D is more than 20L acres which is now 18L acres; the same in state U is 6.5L acres which is now 15 L acres. About 80% of the annual yield from river R is utilized by the farmers of D. It has now come down to 57%. The state U was using 16% now gets 37%. The water received from U by D is 4.57 tmcft during 2010-11; 28.06 during 2011-2012; 135.77 during 2013-2014 and 76.31 during 2014-15. The major cities of U consume drinking water as 26 tmcft by city B; 6 tmcft by city E; the city C of state D consumes 7 tmcft. Present water level at X Dam : 86.94 ft; storage now 44.21 tmcft. Sharp increase in irrigated farm acreage and drinking water use in the state U has deprived D of what it considers its right share. Rainfall in D in September'2016 is high. What should be the water sharing mechanism among states U, D, Y and Z?

Figure 2.4 : Deep Barringer Crater, Winslow, Arizona; Meteriotes

Figure 2.5 : Asteroids, Comets

Test Case : Astronomical Hazards

Prof. Nancy Regon is presenting a test case of astronomical hazards and explores the scope of the aforesaid probabilistic search mechanism (RPSM) to assess and mitigate those threats. The universe is basically a computer, its history is being

computed continuously (Zuse,1967). It is not possible to restrict the occurrence of astronomical hazards; but we have try to protect our earth from total destruction. The astronomical hazards may be really dangerous threats against the sustainability of today's human civilization and the existence of a safe earth. This type of probabilistic search problem is really hard to solve, it is not a trivial problem. Let us discuss the motivation of this threat in details based on the information and images given in figures (2.4,2.5) .

***Asteroids* are the largest of space rocks; most of them circle the Sun in the asteroid belt. Many of 3000 known asteroids are only a few miles across and all of them together would weigh much less than the Moon. Ceres, the largest asteroid, is about 600 miles across; Pallas and Vesta are about 350 miles in diameter. Bright *comets* are visible in the sky only once or twice in a century and stay for many days or weeks. *Meteors* flash in the sky every night or day. Meteor flashes are known as *shooting stars*. But meteors are not stars. Meteors begin as meteoroids in the form of rock or metal that orbit around the Sun. But, sometimes meteoroids plunge into Earth's atmosphere at speeds faster than a bullet. The friction with air particles makes them glow red hot and is called *meteors*. The bright flash is seen for only a few seconds. Perhaps as many as 100 million meteoroids enter the Earth's atmosphere every day. Most are just small pieces of rock and burn in an instant; some become dazzling fireballs and fall to the earth surface called *meteorite*.**

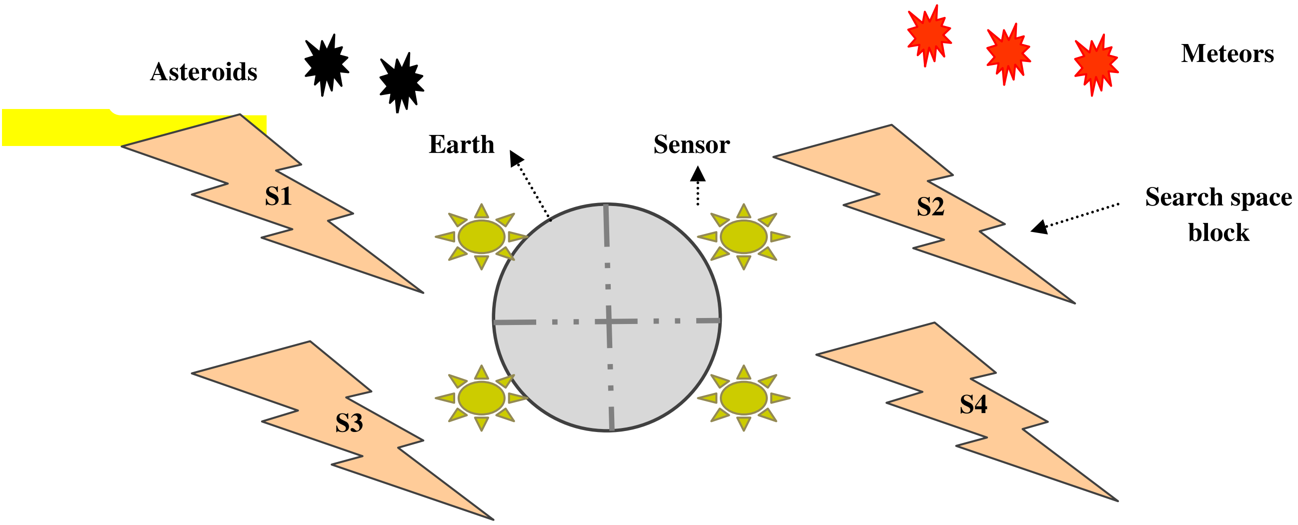


Figure 2.6 : Structure - Astronomical Hazards Detection System

***Problem of astronomical hazards* : Will an or large number of asteroids or a large meteorites ever hit Earth? Many large objects had hit our earth in the past and resulted huge hollows in the ground known as *impact craters*. The largest is the 4150 foot wide and 600 foot deep Barringer Crater near Winslow, Arizona. Is there any probability of mass destruction of human civilization and the earth due to the strike of a comet or the shower of numerous large meteorite or asteroids in future? How to protect our earth from the threat of such type of astronomical hazards? One**

possible solution may be the real-time probabilistic search. The basic objective of the search is to detect the motion of the asteroids, meteors and comet moving dangerously towards the earth in terms of distance, time and size of the objects. The target's position may be uncertain or there may be incomplete information about its size and location. The automated light beam search is expected to be conducted with various types of sensors such as telescopes and satellites. The detection function gives the probability of detection for a search as a function of effort (e.g. search area, distance, time) and evaluates the effectiveness of search efforts in terms of probability of detecting the incoming objects.

Real-time Probabilistic Search Mechanism (RPSM$_{ah}$) :

Agents : **System administrator (Space Research Organization), Human agents;**
Input: **Data stream sensed by the sensors, Rough definition of target, Detection function;**
Output: **Identify objects or moving targets such as asteroids and meteors coming very near to the earth within threshold distance;**
Moves: **Real-time search, group testing, adaptive secure multi-party computation, automated data stream mining by intelligent threat analytics;**
Procedure:
Divide the search space into a set of private blocks;
Assign resources (sensors, satellites, earth station) to each private block; each block is monitored independently; /* the resources of different blocks interact with each other through coordination mechanism and secure broadcast communication protocol (Internet) */;
Project light beam from the sensors on private search space → move forward and backward repeatedly;
Filter data stream;
Detect target → verify correctness to avoid false alarm → call threat analytics → give alert.
Risk Mitigation Strategies**:**

- ***Proactive security*** **(Before astronomical hazards):**
  - **Learn drop-cover-hold**
  - **Have an emergency kit ready and always carry (if possible).**
  - **Build a disaster proof house as per the advice of structural or civil engineering consultant; repair deep cracks on ceilings and walls of the house; fix shelves securely to the walls, avoid heavy loading of the rooms.**
  - ***Safe shelter*** **: (a) build artificial caves at critical locations in urban and rural zone; (b) build robust shed on the roof made of steel (Fe) / Al / Tin (Sn) structure;**
  - **Wear robust helmets and jackets**
  - **Give alert through broadcast communication -→ take safe shelter in time;**

- ***Adaptive security*****:**
  - ***Laser beam projection*** **for** ***object decomposition*** **after detection of incoming objects through probabilistic real-time search;**

- **Artificial *collision* of asteroids and meteors, network *traffic congestion* or *traffic diversion* in space**
- **Activate *Antenna* for blocking and throttling (i.e. slowing speed) of incoming objects entered into the earth based on the principle of electromagnetic induction;**
- **Divert the traffic to the desert or remote zone to minimize the negative impact of astronomical hazards.**
- **During astronomical hazard**
    - **Remain calm and do not panic.**
    - **Take shelter under a table, cover head with hands and hold the table till the hazards last;**
    - **If you are outside, move towards buildings, trees, walls and poles and take shelter;**
    - **I you are inside a vehicle; pull over in a covered place and remain inside.**
- **After astronomical hazards**
    - **Avoid entering damaged civil infrastructure (residential flats, office buildings, industrial plants).**
    - **Use stairs instead of lifts and elevators.**
    - **If trapped in rubble or damaged infrastructure, sound whistle, clap or shout, avoid lighting matchstick, turn on search lights of mobile phones, tap on a pipe or a wall safely.**

***Adaptive security & dynamic data management* : Our earth may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of intelligent security policies, protocols and mechanisms. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the space in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of the space to protect against and adapt to specific threats before the occurrence of known or unknown types of astronomical hazards. Adaptive security monitors the space in real time to detect anomalies, malicious traffic and vulnerabilities. If a threat is detected, it is essential to counter the threat in various ways. Preventative capabilities allow to create infrastructure, products, processes and policies that can mitigate the astronomical hazards. The detective capabilities should identify those threats in time at minimum impact and not detected by preventative capabilities. Retrospective capabilities should perform in-depth analysis of threats not detected by the detective layer to avoid such types of attacks in future. Predictive capabilities provide alerts about external events and anticipates new types of threats.**

Let us consider the technology associated with adaptive security and dynamic data management for the protection of our earth. Today, it is essential to deploy adaptive security architecture for real-time moving target search. A smart grid

demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent astronomical hazards. Adaptive security is an essential part of solar computing. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach. For example, prevention and detection are traditional approaches to the security of our earth. In today's universe of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques for the protection against astronomical hazards.

Dynamic data management is an effective way to move towards adaptive security architecture. DDM surfaces anomalies and adjusts security controls proactively in near real-time to protect our earth. Adaptive Security with dynamic data management is expected to offer many benefits over traditional security platforms : real-time monitoring of events and traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. This technology is expected to adapt to the needs of the system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of the security of our earth with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

5. STRATEGY

Strategy Analytics

***Agents*: System analysts, business analysts, scientist, engineers, technology management consultants;**

Strategic moves

- ✪ **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements (scope, system, structure, security, strategy, staff-resources, skill-style-support);**
- ✪ **Define a set of security goals and emerging technologies accordingly.**
- ✪ **Do technology life-cycle analysis on 'S' curve : presently at emergence phase of 'S' curve.**
- ✪ **Explore technology innovation-adoption-diffusion strategy.**
- ✪ **Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.**
- ✪ **Adopt '4E' approach: envision, explore, exercise and extend.**

Prof. Gramy Woods and Prof. Helen Fisher are presenting on strategy of technology innovation, adoption and diffusion of emerging technologies against natural disaster. The expert panel have explored a set of interesting strategic moves for the innovation, adoption and diffusion of emerging technologies to tackle various types

of natural disaster. It is essential to innovate dominant design of intelligent systems, machines and tools at optimal cost. Most of the technologies are at emergence phase of S-curve. The expertpanel are analyzing strategy of emerging technology innovation in terms of R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovations are closely associated with various strategies of learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of this innovation today.

Rain plays an important role in global economy and the yield of agriculture. But, it is a natural phenomenon and it does not fall as and when we needs it. Triggering rain on demand is an old dream of mankind, with a huge potential socio-economical benefit. It is an interesting research agenda to do SWOT analysis on various methods of artificial rainfall. Traditionally, artificial rainfall is created through cloud seeding method by spraying different chemicals such as silver iodide, calcium chloride or sodium chloride from the aircrafts in the cloud region. Nucleation starts on these chemicals, which lead to the precipitation and then rain. This process has been experimented in South Africa, Thailand, Japan, Mexico, Brazil and some parts of India. The reliability and consistency of the method is low; the risk of failure is high; the cost is also high; it may have negative impact on human society, plants, animals and nature from the perspective of environmental pollution since sprayed chemicals come to the earth along with the rain. Laser induced rainfall is comparatively more economical and reliable method having less pollution and applicable to both white and black clouds. But it is a new method based on the research that self-guided ionized filaments generated by ultra-short laser pulses are able to induce water-cloud condensation in the free, sub-saturated atmosphere at altitude between 45 and 75 m. In this method, a high power pulse laser creates a bunch of filaments or low resistance path between lightning cloud and the earth.

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, shared vision and goal, learning curve, technology life-cycle analysis, technology diffusion and knowledge management strategy. At present, the technology of artificial rainfall is at emergence phase of S-curve. We need fast diffusion of this technology globally to fight against flood and droughts. It is possible to explore different strategic moves for efficient water management; this is basically a natural resource planning (NRP).

- **Natural rainfall control thorough green plantation, conservation of forests and rational rural and urban development planning against building of concrete jungles by cutting trees and plants at mass scale;**
- **Artificial rainfall such as weather modification, rain enhancement through cloud seeding, glaciogenic seeding, hygroscopic seeding and laser induced rainfall;**
- **Transportation of water by rail and truck to the zone with water scarcity;**
- **Save water bodies through pollution control;**
- **Develop smart water grid and irrigation system;**

- **Rational storage, distribution, recycling and reuse of water;**
- **Demand and supply management through capacity utilization, drainage system, water irrigation system and smart water grid;**
- **Collaborative intelligence in water sharing among multiple entities (e.g. districts, states, countries).**
- **Intrusion and migration control of refugees**
- **Restrict wastage of water in swimming pools, water parks, luxurious use of air conditioners and air coolers, by the rich and super rich classes; tap at roadside, leakage from pipelines and construction works.**

Save water bodies **: It is essential to adopt multi-dimensional strategies to save existing water bodies such as intelligent and rational capacity utilization of water from both artificial and natural rainfall; efficient water storage in lakes, ponds, reservoirs, water distribution channels and canals; desalination of sea water; restrict wastage of water in swimming pools, water parks, luxurious use of air conditioners and air coolers, by the rich and super rich classes; tap at roadside and leakage from pipelines; conservation of water to tackle flood and drought, water pollution control (e.g. tube well equipped with water purifier, filter at pumping stations), cleaning of drainage system and riverbed deepening, mutual agreement and dialogue, restriction of illegal encroachment of water bodies, dredging of rivers or canals, collaborative planning, forecasting and replenishment and banning restriction on natural flow of water in river, canals, seas and ocean across borders or boundaries.**

Demand & supply management**: It is essential to estimate the gap between demand and supply of water for a specific zone (e.g. district, state, country). The demand plan is estimated considering various application domains such as agriculture, industries (e.g. manufacturing plants, retail outlets, life-science industry), construction projects, energy (e.g. power plants), drinking water consumption (e.g. mineral water, fruit juice, beverages, soft drinks), cooking food, washing and cleaning of bodies, garments and cars, religious and cultural events (e.g. marriage, parties), entertainment (e.g. swimming pool, sports and games events, infrastructure and ground maintenance), service sector (e.g. education institutes, student's hostels, healthcare institutes, hospitals, offices of private and public sectors, banks and financial services, communication, IT firms, travel and hospitalities, hotels, restaurants) and miscellaneous purposes like transport and logistics services, workshops, seminars, conferences, administration and governance. The supply plan is estimated based on real-time data on natural and artificial rainfall, inflow and outflow of water in a river, availability of water in the reservoirs, wastage or loss due to pollution and disposal of water through drainage system.**

Collaborative intelligence**: Let us first explain the problem of resource allocation and sharing among multiple entities. It is basically a problem of supply chain management. Let us first consider the concept of supply chain in manufacturing sector. Then, the concept can be extended to river water sharing mechanism. Typically, a supply chain is a network of organizations that satisfies the demand of**

ultimate customers by producing values in the form of products and services. Supply chain management is a novel management paradigm; the basic objective is to improve the competitiveness of the supply chain and to fulfill ultimate customer demands by integrating a network of organizational units through systematic coordination of material, information and financial flows. A supply chain includes all the stages involved directly or indirectly in a business process - suppliers, manufacturers, distributors and customers. Each stage performs different processes and interacts with other stages of the supply chain; there is a flow of material, information and funds between different stages. The ultimate objective is to maximize the value, which is measured in terms of the difference between revenue generated from the customer and. the overall cost across the supply chain. In case of river water sharing, a supply chain is a network of upstream and downstream states or countries that satisfies the demand of water of consumers (e.g. agriculture, industrial plants, common people). It is essential to integrate and coordinate the flow of water among various entities through appropriate infrastructure such as distribution channels, irrigation system, dams, storage and drainage system.

Integration of organizational units and coordination of flows of material, information and funds are the basic building blocks of supply chain management. A lack of coordination occurs if information is distorted as it moves across the supply chain or if different stages of the supply chain focus on optimizing their local objectives. The phenomenon in which demand variability is amplified as one moves up the supply chain is known as Bullwhip effect. There are five main causes of Bullwhip effect – error in demand forecasting, high lead-time, batch ordering, supply shortage and price variations. This problem moves the partners of the supply chain away from the efficient frontier and results in a decrease of profitability and quality of service. It is essential to define frameworks for tighter integration and improved coordination of business processes along the supply chain. Successful integration depends on three factors - choice of partners, inter-organizational collaboration and leadership. Effective use of information and communication technology, integration of advanced planning system and enterprise resource planning (ERP) system and process orientation ensure improved coordination of flows in the supply chain. There are various domains of resource allocation in real world such as river water sharing among various states or countries, bandwidth allocation in communication sector, energy flow in a smart grid, budget allocation and typical supply chain management in manufacturing and retail industry. Let us explore how to extend the aforesaid concept of supply chain management to river water sharing between upstream and downstream states. In case of river water sharing, a lack of coordination and disputes occur if information is distorted as it moves across the supply chain or if different stages of the supply chain focus on optimizing their local objectives of demand and capacity utilization. For example, an upstream state may be reluctant to share water with the downstream state.

Collaborative intelligence is an emerging field of artificial intelligence which is focused on human computer collaboration. It is the basic building block of the proposed resource sharing mechanism. Let us first define collaborative intelligence. It supports supply chain collaboration. Collaborative planning, forecasting and replenishment (CPFR) is a strategic tool for comprehensive value chain

management of an organization; this is an initiative among all the stakeholders of the supply chain in order to improve their relationship through jointly managed planning, process and shared information [4]. The ultimate goal is to improve a firm's position in the competitive market and the optimization of its own value chain in terms of optimal inventory, improved sales, higher precision of forecast, reduced cost and improved reaction time to customer demands. Information technology allows supply chain partners to interconnect, but trust is also important. The interplay between trust and technology encourages the commitment of collaboration among the organizations. The partners of a supply chain are often reluctant to share their private information. What has remained the open issue is how privacy can be ensured in exchange of strategic information for collaborative supply chain planning. In case of river water sharing, supply chain collaboration is essential for efficient demand and supply management.

Collaborative intelligence is achieved through multi-party negotiation. Negotiation is a means for a group of decision-making agents to reach mutually beneficial agreements through communication and compromise. It is an important conflict management and group decision-making technique by which a joint decision is made by the agents who cannot achieve their objectives through unilateral actions. They exchange information in the form of offers, counter-offers and arguments and search for a consensus. A wise agreement resolves the conflicting interests of the community fairly and is durable. Negotiation methodology has two key components – negotiation process and negotiation protocol. Multi-party negotiation is a group decision-making process having five distinct phases. The negotiation process starts with the planning phase. The agents initiate several joint activities by specifying their objectives, preference, aspiration and reservation levels and communication mode. Next, they set various agenda such as negotiation protocol, the timing of exchange, deadline, priorities and constraints. Then, they exchange offers and arguments; learn about the limitations of other agents; identify the areas of agreement and disagreement and modify negotiation strategies. Next, they develop joint proposals by relaxing their individual limitations and reach an agreement. Finally, the agents analyze the compromise proposals at conclusion phase and may explore the scope of possible improvements.

The negotiation protocol is a formal model which defines a set of rules to govern the processing of a negotiation support system and related communication and specifies permissible inputs, assumptions, actions and constraints. A protocol can be evaluated on the basis of different perspectives such as computational efficiency, communication efficiency, individual rationality, distribution of computation and pareto efficiency. Distribution of computation is necessary to avoid the problem of a single point of failure. An efficient negotiation mechanism enables the agents to reach a Pareto optimal solution by decreasing the cost of negotiation.

Negotiators are the decision-making agents involved in the negotiation process; the other interveners are mediator, arbitrator, facilitator and rules manipulators. The mediator acts as an impartial agent and guides the negotiators to reach an agreement. The arbitrator may generate a solution on the basis of facts and arguments; the rules manipulator can alter the rules of the negotiation.

Collaborative intelligence in resource allocation is associated with efficient collaborative supply chain planning. Planning is defined as a rational, structured decision making process which aims to find the best choice of objectives and measures to a decision situation and its environmental setting. The coordination of operations along the supply chain requires well structured planning processes. In case of collaborative supply chain planning, two or more local planning domains collaborate through sharing of relevant information in order to create a common and mutually agreed upon plan. It has five strategic moves - domain planning, data exchange, negotiation & exception handling, execution and performance measurement.

Collaborative intelligence is associated with efficient and intelligent supply chain contract such as swing option. Swing option is a specific type of supply contract in trading of stochastic demand of a resource. It gives the owner of the swing option the right to change the required delivery of resources through short time notice. It gives the owner of the swing option multiple exercise rights at many different time horizons with exercise amounts on a continuous scale. A typical swing option is defined by a set of characteristics and constraints. There are predefined exercise times t_i, $i\in[1,2,..,n]$, $1\leq t_1<t_2<\ldots<t_n\leq T$ at which a fixed volume of d_0 units of computational resources may be obtained. With a notice of specific short period, the owner of the option may use swing right to receive more (up-swing) or less (down-swing) than d_0 at any of n moments. The scheme permits swing only at g out of possible n time moments where $g \leq n$ is swing number constraint. A freeze time constraint forbids swings within short interval of the moments. The local constraints up-swing [α] and down-swing limits [β] define how much the requested demand d_i at time t_i may differ from d_0. There are two global constraints which restrict the total requested volume D within the contract period by maximum total demand (γ) and minimum total demand (λ). The option holder must pay penalty determined by a function ρ for violating local or global constraints. The next section outlines Resource Sharing Mechanism (RSM) based on collaborative intelligence and then applies the concept to a test case of river water sharing dispute.

5.1 Case Study – Wild Bushfire

Prof. Bush and Prof. Alan Border are discussing the following case study. Is it possible to validate the rationality of various strategic moves to control wild bushfire globally? Is it possible to extend this study to tackle the disaster of volcano also?

There was a wild bushfire in Astralia in December'2019 - 28 people dead; 3000 animals dead; is it not a natural disaster and emergency catastrophe? Is it possible to exercise a crazy, wild brainstorming session on the above globally and adopt a multi-objective set of moves to tackle the fire so hot so big so dangerous so awful?

- **Artificial rainfall i.e. slow, steady, substantial shower to extinguish wild bushfire**
    - **Laser induced rainfall**
    - **Cloud seeding using the concept of cloud physics**
    - **Artificial increase of humidity of air**

    - Is it possible to divert direction of strong wind causing fast spreading of bushfire?
    - Is it possible to deploy real-time sense-and-respond system for automated smoke detection?
    - Prediction of wild bushfire : is it possible through broadcast, satellite and mobile communication system (e.g. RFID. GPS)?
- **Collaborative intelligence in technology and operations management**
- **Multi-party collaborative resource sharing in terms of man, machine, material, method and money for automated fire extinguishing system (e.g. spraying CO_2, foam etc.)**
- **Design of fire-proof houses having sufficient distance from forests, storage facilities for harvesting rain and ground water, avoiding combustible building materials such as wood, coal and paper, equipped with effective fire extinguishing system, use of solar water pumps, emergency exit passage.....**
- **Call Threat Analytics :**
    - **Cause-effect analysis on wild bushfire:**
        - **Is it a natural disaster caused by the friction between branches of trees and strong wind?**
        - **Lightning strike – lightning arrester, cactus plants;**
        - **Is it a manmade disaster due to use of fossil fuel by tribal people (e.g. coal, diesel, petrol, fireworks) beside forest, bushes and wood?**
        - **Is it an act of bio-terrorism (refer: Amazon forest fire in 2019 for exploration of oil and gas)?**
        - **Effects :**
            - **Fall of air quality causing health hazards and quality of life**
            - **Damage of assets, properties**
            - **Death of life**
            - **Environmental pollution**
            - **Negative impact on farming, travel and tourism, events (e.g. sports)**
    - **Risk assessment and risk mitigation through evacuation or migration of human civilization from wild bush fire proned zone**
- **Collective intelligence in timely rescue operation and total evacuation from risky zone through deployment of forest workforce, natural disaster management workforce, security work force and army;**
- **Development of wild-life sanctuaries and national parks in existing forests; re-engineering of forests; eliminate the concept of ‘zero forest’ i.e. ‘no bushes, no bushfire’;**
- **Distribution of food, water and beverage to the victims and fire affected animals through mobile patrols;**
- **Strategic alliance in sharing of manpower and brain power trough UN climate change council, World economic forum and innovation councils (e.g. NASA);**

- **Countermeasures against climate change, extreme weather conditions and global warming (1^0C increase each year) by adoption of solar power and electrical and hybrid vehicles; organized movement and public campaign;**
- **Common sense public awareness development through intelligent knowledge management system such as broadcast (free from fake news, lies and conspiracy theory, disinformation campaign);**
- **Ensure a perfect fit among scope, system, structure, security, strategy, staff-resources and skill-style-support.**

5.2 Case Study – Epidemic & Pandemic

Dr. Han and Dr. Gatting are analyzing the following case study. Is it possible to adopt a set of intelligent strategic moves rationally to fight against epidemic and pandemic outbreak globally? The basic objective is to develop an *artificial immune system*. The objective of the strategic moves is not to create any unnecessary panic. Rather, we need a rational, optimal mix of proactive and reactive or adaptive approaches for epidemic control in time. It is essential to formulate an intelligent and rational global security policy.

- **Use *alternative workplace* and work from home.**
    - ***Block supply chain* (e.g. food chain, retail chain);**
    - ***Block HR chain***
        - ***Inflow of agents* (e.g. students, researchers, traders, tourists) from foreign countries to the centre of epidemic**
        - ***Outflow of agents* from the centre of epidemic to foreign countries**
- ***Social distancing* : which is correct practice – social distancing or physical distancing?**
    - ***Contact isolation* (e.g. man to man, man to animals), pressure isolation, use of masks, /* use of masks for long duration may result respiratory problems as individuals intake CO_2, the byproduct of their own respiration */**
    - ***Socially responsible initiatives*: socially etiquette and responsible behavior: hand shaking, coughing and sneezing, use of handkerchiefs and shoes; Precautions in washing raw meat and cooking meat (e.g. beef, chicken, pork, mutton, cockroaches, snakes, pangolins); restrict spitting on roadside, use of UV light inside room;**
- ***Quarantine* of virus infected agents in special camps;**
    - ***Border seal* between neighboring countries;**
    - **Restriction on logistics i.e. transport through surface (e.g. car, bus, truck, train, metro rail), water (e.g. ship, steamer, boat) and air (e.g. plane, chopper, helicopter);**
    - **Flaws in scanning and detection of infection by *thermal scanners* at ports and air ports:**
        - ***False positive and false negative errors*;**
        - ***Lock down infected cities*;**
- **Develop AIS (*Artificial Immune System*) based on**
    - ***Danger signal sensing***

  - *Self-nonself classification*
  - *Clonal selection* :
    - *Hotspot*
      - *Containment area* /* Home delivery of medicine, food and essential items; shop and market shut down, total lockdown */
    - *Cluster*: red, orange and green zone; /* based on spread of infection rate, number of testing, feedback of inspectors and high population density in slum area */
  - *Micro-planning*
- *Medical precautions* :
  - What is the method of diagnosis and trial at mass scale!
  - Use of *mask* (e.g. normal, N95, N97), hand gloves, gowns, jackets; cleaning agents to wash hands and faces frequently, /* Is use of mask safe for human health? An agent may inhale CO and CO_2 which are byproductcts of own respiration blocked by mask. */
  - *Pathological test* of saliva, nasal secretion, blood, urine, stool of suspected agents,
    - *PCR (Polymerised Chain Reaction)* : Step 1 - Pan Corona PCR; Step 2- N Covid test /* Severe acute respiratory illness, fever, cold cough or influenza*/
    - *Pool Polymerize Chain Reaction (PPCR)* /*To test the spread of infection in orange and green zone*/
    - *Rapid Antibody Test* : Influenza infected agents in Hotspot zone;
    - Nonavailability of good *quality test kits* and masks; quality problems of masks;
    - *Overpopulation* and high population density in urban slum areas;
    - *Comorbidity* : High risk of death of patients of critical diseases (e.g. cancer, kidney failure), accidents and other mishaps;
    - Is there *death audit committee* during epidemic outbreak?
    - Precaution against *mental depression* (e.g. domestic violence, boring feeling and psychological tension) through yoga, free hand exercises and meditation, positive thinking, collaboration and social works;
    - Nonavailability of special care for critical patients (e.g. cancer, kidney failure, dialysis, diabetes) : Assign top priority to critical care; defer plan of surgical operation of non-critical patients.
    - *Denial-of-Service* in healthcare service due to panic of infectious epidemic and *out-of-stock* situation of essential medicines at retail outlets.
  - Fast innovation *of vaccines* through collaborative R&D by skilled agents; how to ensure security and safety of healthcare professionals;

- ***Artificial climate change*** **in terms of temperature, pressure and humidity for controlling spread of infection;**
- **Intelligent *broadcast communication* through radio and TV channels; caution: exaggeration and overreaction, rumors, propaganda;**
- ***Collaborative intelligence*** **in global scientific research and innovation, technology and operations management**
    - ***Multi-party collaborative resource sharing*** **in terms of *man*, *machine* (e.g. use of drones for spraying disinfecting agents, medicines, food and beverages), *materials* (e.g. shortage of beds, medicine disinfection and cleaning agents), *method* and *money* for epidemic control;**
- **Call *Threat Analytics* → do cause-effect analysis on epidemic;**
    - ***Effects***
        - **Fall of air quality causing health hazards and quality of life,**
        - **Death of life;**
        - **Rapid infection; uncertainty in direction of epidemic spread,**
        - **Environmental pollution; Negative impact on industries (e.g. travel, logistics, education, retail, event mgmt.),**
        - **Recession;**
    - ***Risk assessment*** **and *risk mitigation* through evacuation or migration of human civilization from epidemic proned zone**
- ***Collective intelligence*** **in timely rescue operation and total evacuation from risky zone through deployment of healthcare workforce, security and transport work force and army;**
- **Development of *quarantine camps*, speciality hospitals for epidemic and infectious diseases;**
- **Distribution of food, water and beverage to the victims through *mobile patrols*;**
- ***Strategic alliance*** **in sharing of manpower and brain power through WHO, UN, Red cross, UNICEF and UNESCO;**
- **Countermeasures against *climate change*, *extreme weather conditions* and *global warming* (1^0C increase each year) by adoption of solar power and electrical and hybrid vehicles; organized movement and public campaign;**
- ***Common sense public awareness*** **development through intelligent knowledge management system such as broadcast (free from fake news, rumors, lies and conspiracy theory, disinformation campaign);**
- ***Secure multi-party interaction*** **in *G2C communication*:**
    - ***Level 1 [goal setting]:*** **Fairness, correctness, rationality, sustainability, stability, transparency (regulatory compliance vs. freedom of expression), accountability, trust, commitment;**
        - **Who are the customers? What should be the products and service offerings? How to add real positive values in products or service offerings? How to ensure quality assurance in offerings?**
    - ***Level 2 [Multi-party corruption]:*** **in business model innovation, goal setting, governance, policy formulation on economic affairs, budgeting and system administration, racism, conspiracy theory;**
    - ***Level 3 [System performance audit]:*** **Reliability, consistency, stability, liveness, safety, deadlock freeness, reachability, resiliency;**

    - *Level 4 [Malicious attacks]:* **Sybil, false data injection, shilling, coremelt, DoS (Denial of Service) attack, bioterrorism, medical ragging; is the corona panic really outcome of genetic engineering? /* DoS : nonavailabilty of beds in general hospitals and speciality clinics for epidemic patients.*/**
    - *Level 5 [Access control]:* **authentication, authorization, correct identification, privacy, audit, data integrity, confidentiality and nonrepudiation;**
- **Ensure a perfect *fit* among scope, system, structure, security, strategy, staff-resources and skill-style-support in corporate governance and law and order conrol; coordination and integration among foreign affairs, home affairs, health and family welfare, defense and logistics ministries of all countries.**

6. STAFF-RESOURCES

Staff-resources Analytics

do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- ✪ **Man (human capital management [scientists, business analysts, system analysts, project managers, engineers]: talent acquisition, talent retention, training, reward and recognition;**
- ✪ **Machine (tools, computer hardware, software, internet);**
- ✪ **Material (steel, almunium, copper, building masterials – cement, sand, stone, glass, wood);**
- ✪ **Method (process innovation for disaster management);**
- ✪ **Money (optimal fund allocation, project management, resource allocation, resource distribution).**

Mr. Hansie Rabada and Prof. Rina Bell are presenting the need of staff and other various types of resources for the innovation of emerging technologies. Optimal planning and capacity utilization of various types of resources is essential for promoting best practice in disaster management. The expert panel have identified five critical resources for the innovation of emerging technologies for disaster management - man, machine, materials, method and money. The technologies should support process innovation in disaster operation management. It is essential to train and educate the staff on new technogies -how to operate intelligent automated machines, how to install intelligent systems in cost effective ways. The most critical issue is management of financial resources for the innovation and promotion of new technologies. It is rational to use ERP system for optimal planning and capacity utilization of resources; it is an interesting option to explore ERP system for materials management, HR management, financial and cost control for the innovation of emerging technologies.

The technological innovation related to artificial rainfall demands the commitment of creative talent from the domains of earth science, cloud physics, space research organization and ministry of water resource management. It is crucial to analyze dynamics of the technological innovation in terms of sources of innovation and roles of organizations, government and collaborative networks; fair and correct resources

allocation for effective technological evolution and diffusion, dominant design factors and commitment of creative people. Prof. Pal has recommended an intelligent resource sharing mechanism.

Water Sharing Mechanism (WSM)

Agents: Country or state - B and S; /* There may be multiple parties i.e. countries or states involved in water treaties*/

Input:

- ♦ Analytics for exception handling: Real-time online data on rainfall, inflow and outflow of water in a river;
- ♦ Availability of water in the reservoirs;
- ♦ Demand plan of water for agriculture, drinking and other purposes;

Output : Collaborative water resource sharing plan or delivery plan (P^d);

AI Moves :

- ✓ collaborative intelligence through domain planning, data exchange among planning domains, multi-party negotiation, exception handling, delivery execution and performance measurement.
- ✓ The agents negotiate a swing option contract in terms of
    - fixed base demand (d), local constraints : up-swing (α) and down-swing limits (β);
    - global constraints : maximum total demand (γ) and minimum total demand (λ);
    - penalty (ρ) for violating local or global constraints and
    - swing number constraint (g)
- ✓ Intelligent and rational resource capacity utilization [Reference : section 2.3]

Protocol:

- ▪ Develop front end agreement by forming association.
- ▪ Define joint water sharing plan.

  Negotiation issues:

    - primary : delivery plan;
    - secondary : swing option ($d,\alpha,\beta,\gamma,\lambda,\rho,g$);

  S bids its optimal delivery plan P_o to B.

  Set i = 0. Reference plan = P_o;

  Repeat until the stopping criteria is satisfied:

  Set i = i + 1;

  B counter bids P_i^B to S or S counter bids P_i^S to B;

  $N^s(t, P^t_{i,B\rightarrow S})$ = quit if $t > T^S$ or
  accept offer if $u^S(t, P^t_{i,B\rightarrow S}) \geq u^S(t', P^{t'}_{i,S\rightarrow B})$ or
  counter offer $P^{t'}_{i,S\rightarrow B}$;

  If both parties agree, output plan $P_f = P_i$.

B and S jointly settle the compensation plan to be given to the victim or losing party through negotiation based on final plan $P_{f.}$ in terms of artificial rainfall, cloud seeding, glaciogenic seeding, hygroscopic seeding, rain enhancement, weather modification and water transportation by rail or truck / tanker

- **Create demand forecast plan.**
- **Identify exceptions for demand forecast of water. Call analytics for exception handling.**
    - **demand plan of water**
    - **supply plan of water**
- **Collaborate and resolve demand forecast exception items.**
- **Create the replenishment of order forecast.**
- **Identify exceptions to the order replenishment forecast.**
- **Collaborate and resolve exceptions to the order replenishment forecast.**
- **Create the replenishment order.**
- **Execute delivery plan : allocate and share water.**

Verification principle:

- **verify security intelligence of water allocation and sharing system of the association in terms of**
    - **rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, commitment, reliability and consistency;**
    - **Revelation principle :**
        - **authentication, authorization, correct identification, non-repudiation and integrity,**
        - **audit quality, pollution level and volume of shared water;**
- **verify machine intelligence (M_p) in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy.**

Payment function: verify business intelligence (B_p) in terms of cost sharing, incentive and compensation policy.

Dr. Pal is explaining the water sharing mechanism in depth. Three different classes of agents are involved in the resource sharing mechanism: B, S and mediator (M). B and S have well-defined objective function and a set of constraints that represent their preferences over the possible outputs of the mechanism. These agents act rationally to optimize their objective functions and follow the coordination mechanisms correctly. B and S disclose their negotiated data to M. The primary responsibility of M is to ensure fairness and correctness of resource allocation and sharing.

***Planning domains (Local and Global)*: In case of water sharing, it is hard to define a planning domain based on single or multi-objective optimization; it may be based on a valuation model. Here, B and S hold individual planning domains which are derived from their optimization models; B has a budget constraint and S has a capacity constraint. The agents try to minimize the cost of transaction. The local planning domain of B is defined through the constrained optimization problem: max $(o^B)^T x^B$, s.t. $M^B x^B \leq b^B$ where x^B, o^B, b^B and M^B are the vector of decision variables, the cost vector, the constraint lower bound vector and the constraint matrix for B, respectively (T: matrix transpose operation). Similarly, the lpd of S is: max $(o^S)^T x^S$, s.t. $M^S x^S \leq b^S$. Combining these two one can obtain the joint optimization problem: max $o^T x$, s.t. $Mx \leq b$ where $x = x^B \oplus x^S$, $o = o^B \oplus o^S$, $M=M^B \oplus M^S$ and $b = b^B \oplus b^S$ for the entire system referred as the global planning domain. Here, x, o, M and b represent the set of decision variables, the cost or objective**

function vector, the constraint matrix and constraint upper bound vector for the global plan.

***Plan*: The plan in water sharing is basically a delivery plan of river water. It is a multi-issue negotiation. The bi-party negotiation starts with B bidding a plan P to S. S evaluates P and counter bids an alternative plan P'. B in turn evaluates P' and counter proposes yet another P" and so on. Finally, if the negotiation ends successfully, B and S accept the commonly accepted agreed plan. The negotiation for a plan consists of successive bidding cycles. In each bidding round, a plan P is bid by either B or S. A successful negotiation process consists of an initial plan followed by a series of compromise plans which culminates in a finally accepted plan.**

***Plan utility*: For any plan P, the utility components of B and S are denoted by $u^B(P)$ and $u^S(P)$ respectively. These are private to the agents and will not be disclosed to the opponent, i.e. what is revealed in the negotiation process is the proposal for B and the proposal for S without any utility implications. The total utility for a plan P, $u(P) = u^B(P) + u^S(P)$, is also not revealed to either agent. The concept of utility is also used as plan cost or revenue in artificial intelligence and operations research literature.**

***Local and global utility effects*: Since P_0 is optimal for B, $u^S(P_0) < u^S(P_i)$ for all $i \geq 1$, i.e. the utility effect for B(S) for P_i, $\Delta u^B(P_i) = u^B(P_0) - u^B(P_i)$. $\Delta u^S(P_i) = u^S(P_i) - u^S(P_0)$. Utility effect of B or S is also referred as local utility effect, whereas the global utility effect or total utility effect for P_i is sum of the local utility effects of all the agents. This is because the objective of the coordination process is to increase the total utility, not the individual utility. However, B is entitled to ask for suitable compensation from S to compensate for the reduced utility it has to incur in P_i. Individual utility effects are treated as private information.**

***Compensation and utility sharing*: The losing party will always ask for a compensation amount, which is at least the utility effect. The compensation negotiation has basically two purposes: i) to determine whether the current plan P_i is a feasible one, i.e. whether total utility of P_i has increased over the previous plan P_{i-1} (or any other past plan P_j, $j<i-1$); and ii) to determine how the increased utility to be shared between B and S. This is known as utility sharing.**

Utility implication: Utility Implication of B for a plan P denoted $u'^B(P)$ is the utility component of P, $u^B(P)$ plus the compensation settled $u_m(P)$. Similarly, the utility implication for S agent $u'^S(P)$ is determined. The total of utility implications for B and S is same as the total utility for the plan, u(P). Thus, $u'^B(P) = u^B(P) + u_m(P)$; $u'^S(P) = u^S(P) - u_m(P)$; $u(P) = u^B(P) + u^S(P) = u'^B(P) + u'^S(P)$.

***Compensation negotiation and rational behaviors of the agents* : Incentive or compensation negotiations are realistic. The agents behave rationally. If the total utility increases, compensation will always be settled such that no agent loses compared to the previous round. In other words, the utility implications for both parties improve. Further, if the compensation negotiation fails, it only means that the total utility for the current bid is less than that for the previous bid. When the negotiation ends successfully in the final plan P_f, the total utility achieved is nothing but $u(P_f)$. The total improvement of utility through the negotiation will be $u(P_f) - u(P_0) > 0$, which is apportioned as $u_m(P_f)$ for B and $u(P_f) - u(P_0) - u_m(P_f)$ for S. Both**

B and S are assumed to be rational in exchange of truthful communication and are interested in reducing total plan utility. If none of parties respond then there will be a deadlock. That means that neither B nor S is interested in utility improvement, which violates our assumption. Privacy preservation of individual agents is an important concern for this cooperative game. For this purpose, the utility effects are compared privately. Because the utility effects are kept secret from the respective opponents, the compensation negotiation becomes relevant and the parties feel encouraged to participate in this negotiation. It may be a single or multi-issue negotiation.

***Payment*: The buying and selling agents disclose the pricing, compensation and delivery plans to the mediator. The mediator checks the authenticity of the identities of the agents and regulatory constraints such as ceiling, consent and sustainability clauses; verifies fairness and correctness of valuation and announces penalty clauses against malafide behavior. The mediator computes payment based on disclosed data; collects payment. S collects payment from B.**

***Stopping criteria*: Stopping the mechanism is possible on various counts such as stable preference matching, total negotiation time deadline, total number of plan bidding rounds and number of successive failed biddings. If any agent withdraws prematurely the mechanism ends unsuccessfully.**

***Compensation* : The agents may settle compensation in various ways such as financial budget allocation or incentive sharing or unconventional ways. Let us consider the case of water sharing between two countries or states. B and S jointly settle the compensation plan to be given to the victim or losing party through negotiation based on final plan in terms of artificial rainfall, cloud seeding, glaciogenic seeding, hygroscopic seeding, rain enhancement, weather modification and water transportation by rail or truck / tanker. The upstream state requires additional amount of water for the growth and development in agriculture, industries, power plants and urban and rural planning. Its demand for water has increased and so the inflow of river water to the downstream state has reduced significantly. On the other side, the downstream state requires more water for the growth and development of urban and rural zones, agriculture and industries. The problem is severe during drought in the summer. So, how is it possible to supply more water to the downstream state – the option is artificial rainfall through cloud seeding. In this case, the compensation may not be directly related to fund allocation or financial support from the upstream to the downstream state. Actually, it is expected to be technological support for artificial rainfall. Can we think of cloud computing in the context of artificial rainfall and cloud seeding – how to control the generation and movement of cloud as per the demand of water of a specific zone?**

There are several critical factors associated with fair, correct and rational resource sharing mechanism like river water: good governance, trust, positive mindset, commitment, political will, power play, corporate social responsibilities, cancer of mind, selfish ego, identity crisis and conspiracy for war. Malicious agents always try to sustain the conflict of resource sharing among multiple entities to gain political mileage, incentives from enhanced defense budget and other financial opportunities. War or terrorism may start due to conflict in water sharing. The Supreme Court is expected to act as a Trusted Third Party. A supervisory panel should be set up to

decide quantum of water release after studying online data of rainfall and flow in the river. Central Water Commission (CWC) should define a new protocol of online collection of data related to rainfall and flow of water on real-time basis. The meteorological department's rainfall data and flow into reservoirs of upstream state should match with inspected or verified data. The inflow may be artificially reduced due to unauthorized diversions by a state through various lift irrigation schemes in violation of the final order of the tribunal. It is the duty of the state government to maintain law and order.

The panel have discussed the role of staff-resources for disaster management such as epidemic and pandemic outbreak. The technological innovation on vaccines to fight against new viruses demands the commitment of creative talent from the domains of medical science operations management, managent information systems, healthcare administration and biomedical engineering. It is crucial to analyze the dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion, dominant design factors, effects of timing and mode of entry. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment.

The expert panel have identified five critical resources for epidemic and pandemic control : man (e.g. healthcare staff, nurses, doctors, testing staff, government staff of ministry of healthcare and family welfare, scientists and research staffs of innovation lab), machine (e.g. testing kit, thermal scanner, healthcare infrastructure, camps, hospitals) material (e.g. cleaning agents, sanitizers, masks, gloves, medicine, jacket), method (e.g. process innovation in registration, consulting, testing, broadcasting, governance) and money (e.g. budget allocation for healthcare infrastructure development such as hospitals and quarantine camps, disaster relief fund). 'Man' analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, payment function, compensation, reward, incentive, health insurance of staff and performance evaluation. 'Machine' analyzes the basic aspects of required test kits and medicine of optimal stock. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure. Finally, 'money' highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.

The technological innovation against astronomical hazards demands the commitment of creative talent from the domains of earth science, space research organization and ministry of science and technology. It is crucial to analyze the dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion, dominant design factors, effects of timing and mode of entry. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities,

thinking style, knowledge, personality, motivation, commitment and interaction with environment. Natural disaster is not a trivial problem; it needs useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics.

7. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- ***Skill*: knowledge of operation and best practices of engineering, technical, system administration, strategic management, governance and disaster operation management;**
- ***Style*: leadership, shared vision, goal setting, intelligent communication, risk assessment and mitigation, innovation project management;**
- ***Support* : proactive, preventive and reactive support of systems, machines and tools used for disaster operation management.**

Finally, Prof. Nick Jones, Prof. Gramy Woods and Dr. Hariharan are concluding the session by exploring skill, style and support as required for the innovation of emerging technologies and operation management against natural disaster. The workforces involved in such technological innovation are expected to develop different types of skills in technical, management and system administration. The workforces involved in technological innovation for edidemic and pandemic control are expected to develop different types of skills in medical science, immunology, disaster operation management and system administration, innovation on life-science, pharmacy and biotechnology, research and development, testing, tracing, tracking, benchmarked and standardized medical practice.

The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of top technology innovation requires the support of great leadership style; they are not only industry leaders but also political one. The style is basically the quality of leadership; the great leaders must have passion, motivation and commitment. The leaders must be able to share a rational vision, mission and values related to the innovation among all the stakeholders honestly and appropriately in time. A traditional functionally centered organization model may not be suitable for supporting end-to-end water resource management process. The technology needs the support of a collaborative enterprise model. The stakeholders are expected to develop skills in collaborative planning, forecasting and replenishment (CPFR) practice as follows.

A) Develop front end agreement: The objective is to establish rules and guidelines for a collaborative relationship. The process steps may be as follows : develop

mission statement, determine goals and objectives; discuss competencies, resources and systems; define collaboration points and responsible business functions; determine information sharing needs (what information, frequency, technology), determine service and order commitments; determine resource involvement and commitments; define conflict resolution process; determine process for reviewing the collaborative arrangement and publish front-end arrangement;

B) Joint resource sharing plan : The basic objective is to unerstand each partner needs and capabilities in creating and influencing demand, manufacturing and replenishment. The process steps may be as follows : identify partner strategies; develop category roles, objectives and goals; develop joint category strategies and tactics; develop item management profiles; develop joint resource sharing plans; agree to joint resource sharing plans.

C) Demand forecast creation : The basic objectives are to create a demand forecast that will lead to the creation of the replenishment order. The process steps may be as follows : analyze joint resource sharing plan; analyze causal factors (e.g. seasonality) on demand; collect and analyze point of history or time series data; identify planned events; identify exceptions or forecast disagreements and generate the demand forecast.

D) Identify exceptions for forecast : The basic objective is to using predefined tolerances and metrics, identify exceptions in the demand forecast for collaborative resolutions. The process steps may be as follows : understand and retrieve exception criteria. identify changes and updates; update the system with constrained demand forecast; compare item values to exception criteria and identify exceptions for collaborations.

E) Collaborate and resolve demand forecast exception items. : The basic objective is to resolve exceptions to the demand forecast through collaboration. The process steps may be as follows : identify desired adjustments to the demand forecast; recommend forecast adjustments and agree on the forecast adjustments.

F) Create the replenishment of order forecast : The basic objective is to develop and communicate a time-phased projection of replenishment orders based on demand forecast. The process steps may be as follows : communicate the demand forecast, consider inventory strategies and current inventory levels, analyze manufacturer's historical replenishment performance, analyze and communicate manufacturing capacity limitations, evaluate factors affecting replenishment planning decisions, review execution performance and create order replenishment forecast.

G) Identify exceptions to the order replenishment forecast: The basic objective is to identify replenishment orders based on predefined tolerances and criteria. The process steps may be as follows : understand and retrieve exception criteria; utilize the replenishment order forecast in the sales and operational planning processes; compare the proposed replenishment order forecasts to supply and capacity; apply constraints and capacity optimization factors to the order replenishment forecast; identify exceptions items based on predefined tolerances.

H) Collaborate and resolve exceptions to the order replenishment forecast : The process steps may be as follows - identify and communicate exceptions, recommend order replenishment forecast adjustments and agree on the forecasts.

I) Create the replenishment order : The process steps may be as follows : utilize the planning system to generate and communicate replenishment orders internally and to the trading partners; the final output is the replenishment orders that are in synchronization with the demand forecast and are aligned with the joint resource sharing plan.

J) Delivery execution : Start sharing resources.

8. CONCLUSION

This session has outlined an interesting project for critical resources (e.g. river water) sharing among multiple entities rationally with fairness, correctness, transparency and accountability. It is also essential to control heavy rainfall which often results flood, landslide and soil erosion in urban and rural zone. Such type of project requires the support of deep analytics of river and irrigation engineering, water resource management and cloud physics. Rational resource sharing is basically the problem of real-time supply chain optimization.

It is also a critical research agenda to explore efficient risk mitigation strategies against heavy rainfall and flood. How can we fight against natural calamities like flood due to heavy rainfall? We need an optimal mix of proactive and reactive approaches. Intelligent urban and rural development planning is essential in terms of reliable infrastructures (e.g. houses, roads, bridges, flyover, drainage system etc.). Can we explore the concept of a 'smart water grid' to divert surplus water through pipelines, canals, rivers and drains to neighboring districts or states from flooded zone? It is rational to monitor timely release of water from various dams sequentially during rainy season; simultaneous release of water from all the dams of a state may aggravate the flood situation; it may be a conspiracy to draw flood relief fund by creating chaos through malicious artificial intelligence. Sufficient number of water storage or harvesting systems (e.g. dams) is required.

Modern, well designed networks of drainage systems should be built along with filters. Regular cleaning of drains is essential to remove mud, sand, plastic goods, polythene packets, haggis and pads to avoid congestion or jamming in rainy season. It is also required to open manholes during rain carefully monitored by municipal and cleaning staff so that there should not be water logging problems on the roads and streets. It is an interesting and feasible option to increase level of residential plots at low land using soil and bricks. Intelligent evacuation plan should be ready during natural disaster. Migration of human civilization from risky zone and fair rehabilitation is also essential. The problem should be tackled scientifically; there may be threats of false data injection attacks and rumors such as superstitions, narrow prejudices and religious curses through various broadcast communication channels. The system administrators should be alert of the readiness of natural disaster relief workforce (NDRF) and army with helicopters, choppers, life- boats and other relief equipments during rainy season. It is rational to exercise capital budgeting based on fair and correct valuation by the experts, surveys, audit and demand plan of reliable infrastructure (e.g. road, bridges, flyovers and nano-housing scheme). How can we tackle cloudbursts artificially applying the concept of cloud physics? It is an open research agenda.

It is possible to construct similar type of search mechanism like RPSM and risk mitigation strategies against the threats of geological hazards such as earthquake. For example, the risk mitigation strategies should include rational approaches in urban and rural development planning, public policy making, cautious approach and regulatory compliance on mining of earth's soil (e.g. coal, minerals, sand, gas pipeline) and construction activities (e.g. saturation in metropolitan cities, building high storied buildings without soil testing, tunnels, metro rails, irrigation projects, dams etc.), monitoring of volcanoes and landslides in hilly zones. The aforesaid type of probabilistic search problem is really hard to solve and it is also challenging to deploy RPSM in reality and seeks extensive support, coordination, planning and corporate social responsibilities from various space research organizations and earth science institutes globally. The most critical challenges involve the innovation of automated real-time search algorithm, intelligent sensors and predictive analytics, resource planning and deployment, system administration and coordination both locally and globally. Artificial intelligence is basically simulation of human intelligence. A rational reasoning system often needs the support of an intelligent analytics. An intelligent reasoning system demands new solution methodology beyond traditional knowledge base with imagination, envision, perception and proper assessment of a hard problem like the aforesaid probabilistic search.

FURTHER READING

- **N.Bostrum. 2014. Super intelligence: Path, dangers, strategies. Oxford University Press.**
- **D. Perlis. 2016. Five dimensions of reasoning in the wild. AAAI.**
- **D. Dasgupta (ed). 1999. Artificial Immune Systems and Their Applications. Springer.**
- **D.Dasgupta and F.Gonzalez. 2002. An immunity-based technique to characterize intrusions in computer networks. IEEE Trans Evol Comput 6:1081–1088.**
- **J.D.Farmer, N.H. Packard and A.S. Perelson. 1986. The immune system, adaptation, and machine learning. Physica 22:187–204.**
- **E.Hart and J.Timmis. 2008. Application areas of AIS: the past, the present and the future. Appl Soft Comput 8:191–201.**
- **S.Forrest, A.S. Perelson, L. Allen and R. Cherukuri. 1994. Self–nonself discrimination in a computer. In: Proceedings of the IEEE symposium on research in security and privacy, Oakland, CA, USA, pp 202–212.**
- **S. Hofmeyr and S. Forrest. 2000. Architecture for an artificial immune system. Evol Comput 7:1289–1296.**
- **E.Rich and K. Knight. 1991. Artificial intelligence, 2nd edn. McGraw-Hill, New York.**
- **G.Luger. 2005. Artificial intelligence: structures and strategies for complex problem solving, 5th edn. Addison-Wesley, New York.**
- **A.Cawsey. 1998. The essence of artificial intelligence. Prentice-Hall, Englewood Cliffs.**

- **P. Norvig. 1992. Paradigms of Artificial Intelligence Programming: Case Studies in Common Lisp. Morgan Kaufmann.**
- **S. J. Russell and E. H. Wefalld. 1991. Do the Right Thing: Studies in Limited Rationality. MIT Press.**
- **A. Konar. 1999. Artificial Intelligence and Soft Computing. CRC Press.**
- **J.Kim, P.Bentley, U.Aickelin, J.Greensmith, G.Tedesco and J.Twycross J. 2007. Immune system approaches to intrusion detection - a review. Nat Comput 6:413–466.**
- **P.Matzinger. 1994. Tolerance, danger and the extended family. Ann Rev Immunol12:991–1045.**
- **P.Matzinger. 2001. The danger model in its historical context. Scand J Immunol 54:4–9.**
- **P.Matzinger. 2002. The danger model: a renewed sense of self. Science 296:301–305.**
- **L. Castro and C.J.Timmis. 2002. Artificial Immune Systems : A New Computational Intelligence Approach. Springer.**
- **A.O.Tarakanov, V.A.Skormin and S.P.Sokolova. 2003. Immunocomputing: Principles and applications. Springer.**
- **J.Douceur. 2002. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS).**
- **A.K.Pal, D. Nath and S.Chakraborty. 2010. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor. WASET, Brazil.**
- **S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Indian Institute of Management Calcutta, India.**
- **G.Kol and M.Naor. Cryptography and game theory: Designing protocols for exchanging Information. Proceedings from 5th Theory of Cryptography Conference (TCC), 2008.**
- **W. Du. A study of several specific secure two-party computation problems. Doctoral dissertation, Purdue University, USA. 2001.**
- **Y. Lindell. Composition of secure multi-party protocols a comprehensive study. Springer. 2003.**
- **S.Chakraborty. A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Doctoral dissertation (unpublished), Indian Institute of Management Calcutta, 2007.**
- **A.L.Melnick. Biological, chemical and radiological terrorism. Springer, NY,USA, 2008.**
- **S. Chakraborty. Security intelligence for broadcasts: Threat analytics. Technical report. 2012.**
- **J.Douceur. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS). 2002.**
- **A.K.Pal, D. Nath and Chakraborty, S. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor, WASET, Brazil.2010.**
- **M.Shema. edited by A.Ely. Seven deadliest web application attacks. Elsevier. 2010.**

- **F.A.Kuglin. Pharmaceutical supply chain drug quality and security act. CRC Press, Taylor & Francis Group, Boca Raton, USA.**
- **G.Ateniese, R.Curtmola, B. Medeiros and D.Davis. Medical information privacy assurance: Cryptographic and system aspects, Technical Report, John Hopkins University. 2003.**
- **M.Gertz and S.Jajodia. Handbook of database security applications and trends. 2008.**
- **B. Schneier. Applied Cryptography, John Wiley, New York,1996.**
- **W.Mao. Modern Cryptography Theory & Practice, Pearson Education. 2007.**
- **Y.Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). LNCS 1318, Springer-Verlag.**
- **S.Chakraborty. 2007. A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Thesis, Fellow Programme, Indian Institute of Management Calcutta.**
- **S.Chakraborty and S.K.Sharma. 2007. Enterprise Resource Planning: an integrated strategic framework. International Journal Management and Enterprise Development, vol. 4, no. 5.**
- **G.Dudek and H. Stadtler 2005. Negotiation-based collaborative planning between supply chain partners. European Journal of Operational Research, 163, 668-687.**
- **D.Seifert. 2002. Collaborative planning, forecasting and replenishment. Galliers Business.**
- **S.L.Epstein. 2015. Wanted: Collaborative Intelligence. Artificial Intelligence, 221, 36-45.**
- **R.T.Bruintjes. 1999: A review of cloud seeding experiments to enhance precipitation and some new prospects. Bulletin of the American Meteorological Society: Vol. 80, No. 5, pp. 805-820.**
- **W.A.Cotton and R. A. Pielke. 1995. Human Impacts on Weather and Climate. Cambridge University Press.**
- **R.T. Bruintjes, D. W. Breed, V. Salazar, M. Dixon, T. Kane, G. B. Foote and B. Brown. 2001: Overview and results from the Mexican hygroscopic seeding experiment. Preprints, AMS Symposium on Planned and Inadvertent Weather Modification, Albuquerque NM.**
- **A.C.Cooper, R. T. Bruintjes and G. K. Mather. 1997: Calculation Pertaining to Hygroscopic Seeding with Flares. Journal of Applied Meteorology: Vol. 36, No. 3, pp. 1449-1469.**
- **G.K.Mather, D. E. Terblanche, F. E. Steffens and L. Fletcher. 1997. Results of the South African cloud-seeding experiments using hygroscopic flares. Journal of Applied Meteorology: vol. 36, No. 11, pp. 1433-1447.**
- **B.A.Silverman and W. Sukarnjanaset. 2000. Results of the Thailand warm-cloud hygroscopic seeding experiment. J. Appl. Meteor., 39, 1160-1175.**
- **K. Shivshankar, K.R. Chopkar, A. Gangakhedkar and B.Dhone. 2014. Cloud formation and atmospheric rain making by endothermic reaction due to plasma laser & UV radiation in the atmosphere. International Journal of Information Technology and Business Management, vol.21 No.1.**
- **Qiu, J. & Cressey, D. Taming the sky. Nature 453, 970–974 (2008).**

- **US National Research Council. Critical Issues in Weather Modification Research (National Academies, 2003).**
- **Langmuir, I. Growth of particles in smokes and clouds and the production of snow from supercooled clouds. Science 106, 505 (1947).**
- **Kasparian, J. et al. White-light filaments for atmospheric analysis. Science 301, 61–64 (2003).**
- **Couairon A. & Mysyrowicz, A. Femtosecond filamentation in transparent media. Phys. Rep. 44, 47–189 (2007).**
- **Berge´, L. Skupin, S., Nuter, R., Kasparian, J. &Wolf, J.-P. Ultrashort filaments of light in weakly-ionized, optically-transparent media. Rep. Prog. Phys. 70, 1633–1713 (2007).**
- **Kasparian, J. & Wolf, J.-P. Physics and applications of atmospheric nonlinear optics and filamentation. Opt. Express 16, 466–493 (2008).**
- **Chin, S. L. et al. The propagation of powerful femtosecond laser pulses in optical media: physics, applications and new challenges. Can. J. Phys. 83,863–905 (2005).**
- **Be´jot, P. et al. Higher-order Kerr terms allow ionization-free filamentation in air. Phys. Rev. Lett. 104, 103903 (2010).**
- **Me´jean, G. et al. Multifilamentation transmission through fog. Phys. Rev. E. 72, 026611 (2005).**
- **La Fontaine, B. et al. Filamentation of ultrashort pulse laser beams resulting from their propagation over long distances in air. Phys. Plasma 6, 1615–1621 (1999).**
- **Rodriguez, M. et al. Kilometer-range non-linear propagation of femtosecond laser pulses. Phys. Rev. E 69, 036607 (2004).**
- **Chin, S. L. et al. Filamentation of femtosecond laser pulses in turbulent air. Appl. Phys. B 74, 67–76 (2002).**
- **Salame´, R., Lascoux, N., Salmon, E., Kasparian, J. & Wolf, J.-P. Propagation of laser filaments through an extended turbulent region. Appl. Phys. Lett. 91,**
- **171106 (2007).**
- **Me´chain, G. et al. Propagation of fs-TW laser filaments in adverse atmospheric conditions. Appl. Phys. B 80, 785–789 (2005).**
- **Kasparian, J. et al. Electric events synchronized with laser filaments in thunderclouds. Opt. Express 16, 5757–5763 (2008).**
- **Wille, H. et al. Teramobile: a mobile femtosecond–terawatt laser and detection system. Eur. Phys. J. Appl. Phys. 20, 183–190 (2002).**
- **Kasparian, J., Sauerbrey, R. & Chin, S. L. The critical laser intensity of self-guided light filaments in air. Appl. Phys. B 71, 877–879 (2000).**
- **Pruppacher, H. R. & Klett, J. D. Microphysics of Clouds and Precipitation (Kluwer Academic Publishing, 1997).**
- **Measures, R. M. Laser Remote Sensing—Fundamentals and Applications (Wiley**
- **Interscience, 1984).**
- **Tzortzakis, S., Prade, B., Franco, M. & Mysyrowicz, A. Time evolution of the plasma channel at the trail of a self-guided IR femtosecond laser pulse in air. Opt. Commun. 181, 123–127 (2000).**

- **Braun A., Korn G., Liu X., Du D., Squier J. and Mourou G., (1995) Self-channeling of high- peak power femtosecond laser pulses in air, Opt. Lett. 20, 73-75.**
- **Mason B.J., (1975) Clouds, Rain and Rainmaking, Second Edition, Cambridge University Press, Cambridge.**
- **Mason B.J., (1971) The Physics of clouds, Second Edition, Calare don Press, Oxford.**
- **Mejean G., Ackermann R., Kasparian J., Salmon E., Yu J., Wolf J. -P., Rethmeier K., Kalkner W., Rohwetter P., Stelmaszczyk K. and Woste L., (2006) Improved laser triggering and guiding of megavolt discharges with dual fs-ns pulses, App. Phys. Letts., 88, 021101-3.**
- **Rohwetter P., Kasparian J., Stelmaszczyk K., Hao Z., Henin S., Lascoux N., Nakaema W. M., Petit Y., Queisser M., Salame R., Salmon E., Woste L. and Wolf J. -P. (2010) Laser-induced water condensation in air, doi: 10.1038/nphoton.2010.115.**
- **Wallance J.M. and Hobbs P.V., (1977) Atmospheric Science, Academic Press, London**
- **Yoshihara K., Takatori Y., Miyazaki K. and Kajit Y., (2007) Ultraviolet light-induced ter- droplet formation from wet ambient air, Proc. Jpn. Acad. Sci. B 83, 320-325.**
- **S.S.Brown. 1980. Optimal search for a moving target in discrete time space. Operations Research, volume 28, no. 6, pp. 1275-1289.**
- **T.Ishida. 1992. Moving target search with intelligence. AAAI-92, pp. 525-532.**
- **E. Kagan and I. Ben-Gal. 2013. Moving Target Search Algorithm with Informational Distance Measures. Entropy.**
- **P. J. Schweitzer. 1971. Threshold Probabilities when Searching for a Moving Target. Operations Research, 19(3), 707–709.**
- **J. N. Eagle. 1984. The Optimal Search for a Moving Target when the Search Path is Constrained. Operations Research, 32, 1107–1115.**
- **L. C. Tomas and J. N. Eagle. 1995. Criteria and Approximate Methods for Path-Constrained Moving-Target Search Problems. Naval Research Logistics, 42, 27–38.**
- **D. A. Grundel. 2005. Searching for a Moving Target: Optimal Path Planning. IEEE Conference on Networking, Sensing and Control, 19–22 March, 2005, 867–872.**
- **I. M. MacPhee and B. P. Jordan. 1995. Optimal Search for a Moving Target.**
- **A. Stenz. 1994. Optimal and Efficient Path Planning for Partially-Known Environments. IEEE International Conference on Robotics and Automation, San Diego, CA, USA, vol. 4, 3310–3317.**
- **A.Jaszkiewicz and R.Slowinski. 1999. The light beam search approach an overview of methodology and applications. European Journal of Operational Research, 113, 300-314.**
- **S.Simon. 1998. Comets, meteors and asteroids. Scholastic Inc.**
- **W.Du and M. J. Atallah. 2001. Secure multi-party computation problems and their applications: a review and open problems. In 2001 workshop on new security paradigms (pp. 13 - 22). ACM Press.**

- **Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.**
- **R.Canetti, U.Feige, O.Goldreich and M.Naor. 1996. Adaptively secure multi-party computation.**
- **S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. IIMC.**

Quiz

- **What are various types of natural disasters? What are the negative impacts of such disasters on poverty and humanity, plants, animals and nature? What is the scope of technology for global security against various types of disaster such as flood, drught, storm, earthquake, volcano, woodfire, snowfall, epidemic and pandemic outbreak, astronomical hazards, environmental pollution and attack of malicious pastes and wild animals?**

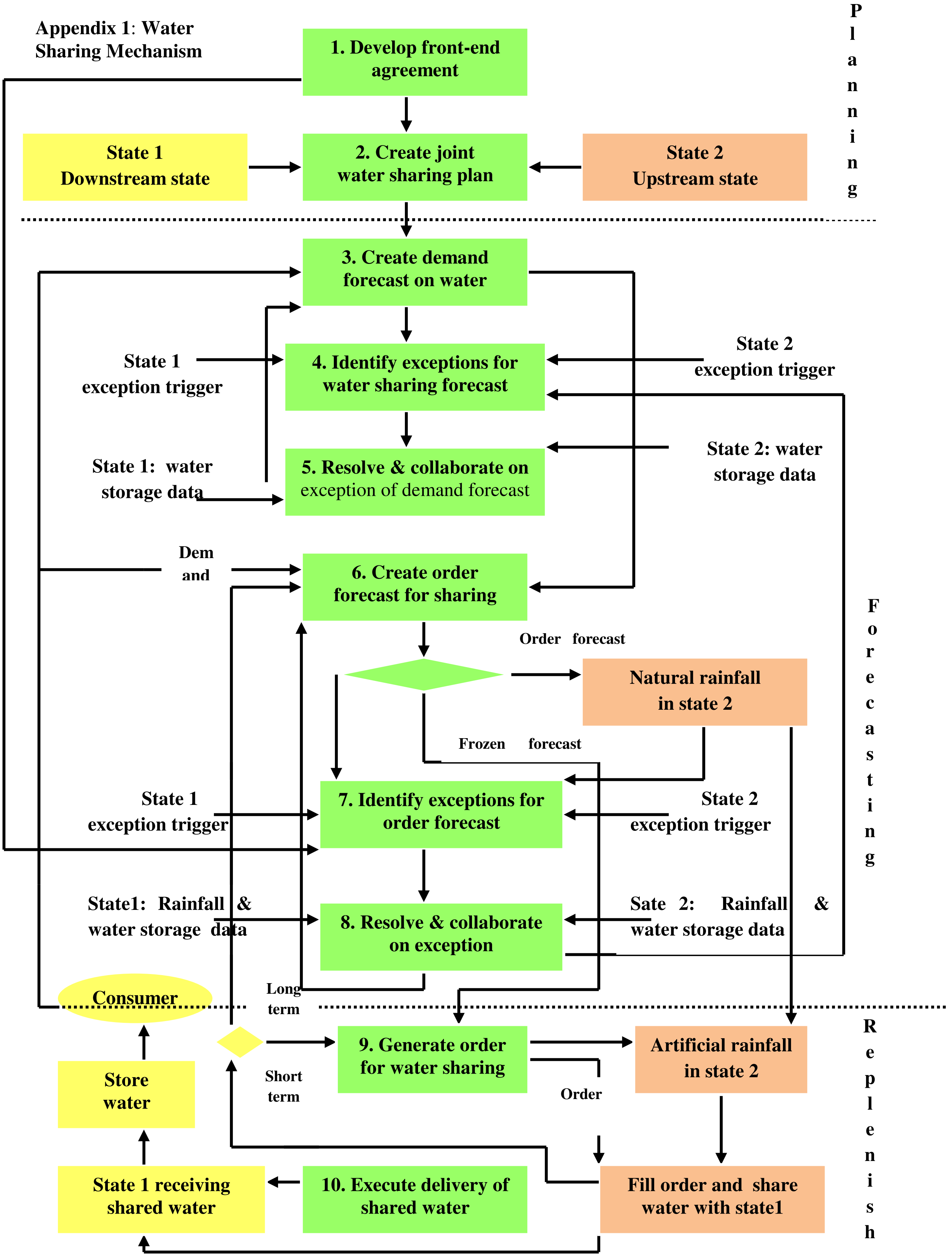
/* Hints :
***Flood* : Smart water grid, Canals, Drainage system, Irrigation system, Water storage system (e.g. dams, lakes, ponds, rivers), Migration of human civilization from risky zone to favourable zones**
***Drought* : Artificial rainfall, Cloud seeding, Irrigation system, Water storage system, Fertilizer and Migration of human civilization from risky zone to favourable zones.**
***Storm / Cyclone* : Resiliency management, Infrastructure maintenance (e.g. energy, utilities, trees, huts, houses)**
***Earthquake* : Soil mining, Tunnel, Unplanned urban and rural development planning and civil infrastructure development, Migration of human civilization from risky zone to favourable zones**
***Volcano* : Migration of human civilization from risky zone to favourable zones**
***Wood fire* : Water jet, Artificial rainfall, Migration of human civilization from risky zone to favourable zones**
***Snowfall* : Resiliency, traffic congestion**
Epidemic and pandemic outbreak
***Astronomical hazards* : Private search**
***Environmental hazards* [Air pollution (Smoke from vehicles, power plants, industrial plants (e.g. chemical, metallurgical, fertilizers, oil, gas), factories); Water pollution: cleaning of weeds i.e. kachuripana, Soil pollution: plastic, garbage, recycle and reuse; Sound pollution : fire crackers, bombs, construction works, industrial plants and factories; Sunlight pollution : Nano-housing]**
***Paste / wild beasts* : Mosquitoes - Malaria, dengue, chickengunia (Mosquito net, DDT, Bleaching powder, Cleaning of garbage) ; Flies : food poisoning (use covers; no animal husbandries (e.g. khatals – cows, buffaloes, goats) and poultry firms in urban zone); Attacks of wild animals, Wild-life sanctuaries (e.g. tigers, loans, elephants, snakes, rhinos, hippopotamus, lions, monkeys, baboons), Conservation of forests and cleaning of bushes. */**

  - **What is artifial immune system? How can it control epidemic and pandemic outbreak?**

- **What are the basic elements of system architecture for disaster control? How to represent the structure correctly?**
- **What do you mean by technology security for artificial immune system? How to verify the security intelligence? What is bioterrorism? How to assess and mitigate risks of bioterrorism globally?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis?**
- **How to manage resources for disaster management? What should be the talent management strategy?**
- **What are the skills, leadership style and support demanded by the technological innovation?**
- **How to manage technology innovation project efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements for disaster management?**
- **Explain the problem of real-time moving target search? Justify it as a technology for humanity. What is the scope of this technology for the protection of our earth against astronomical hazards?**
- **What is the dominant design of the technology?**
- **What are the basic elements of the system architecture? How to represent the structure correctly?**
- **What do you mean by technology security for real-time moving target search? How to verify the security intelligence? What is the role of adaptive security and dynamic data management in this context? Design adaptive security architecture.**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis?**
- **How to manage resources in this innovation project? What should be the talent management strategy?**
- **What are the skills, leadership style and support demanded by the technological innovation?**
- **How to manage technology innovation project efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements?**
- **What is private search? Please do the complexity analysis of private light beam search based on multi-objective optimization?**
- **Construct a real-time moving target search algorithm for robot navigation. Please do the complexity analysis.**
- **Explain the technology of artificial rainfall? Justify it as a technology for humanity. What is the scope of this technology for the protection against drought and flood?**
- **What is the dominant design of the technology? Is it possible to adopt laser induced rainfall?**

- **What are the basic elements of the system architecture? How to represent the structure correctly?**
- **What do you mean by technology security? How to verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis?**
- **How to manage resource sharing rationally for this innovation project? Develop a collaborative resource sharing mechanism to resolve the conflicts of water distribution among two neighboring states or countries.**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How to manage technology innovation project efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements?**

Appendix 1: Water Sharing Mechanism


Planning
1. Develop front-end agreement
State 1 Downstream state
2. Create joint water sharing plan
State 2 Upstream state
3. Create demand forecast on water
State 1 exception trigger
4. Identify exceptions for water sharing forecast
State 2 exception trigger
State 1: water storage data
5. Resolve & collaborate on exception of demand forecast
State 2: water storage data
Demand
6. Create order forecast for sharing
Order forecast
Natural rainfall in state 2
Forecasting
Frozen forecast
State 1 exception trigger
7. Identify exceptions for order forecast
State 2 exception trigger
State1: Rainfall & water storage data
8. Resolve & collaborate on exception
Sate 2: Rainfall & water storage data
Consumer
Long term
Short term
9. Generate order for water sharing
Artificial rainfall in state 2
Order
Replenish
Store water
State 1 receiving shared water
10. Execute delivery of shared water
Fill order and share water with state1

SESSION 3: FOOD & HOME SECURITY - SMART AGRICULTURE, NANOHOUSING, SMART VILLAGES & SMART CITIES

***Event* : Technology for humanity and global security summit;**
***Venue*: Social security hall, Technology park : Sanada;**
***Time* Schedule : 3 p.m. – 6 p.m., 15.8.2020;**
***Agents* : Representatives of various global organizations, World bank, Global Economic forum, Technology management experts from science and technology forums, agriculture, textile, civil, structural, mechanical and chemical engineers, scientists, representatives and ministers from the departments of agriculture, consumer goods and housing.**
***Topic of discussion and key focus areas*: Food security, home security, garments security, consumer goods security, organic farming, smart farming, agricultural engineering, nano housing, textile engineering;**
***Keynote speakers* : Prof. Boris Zekov, Dr, Hansie Kallis, Dr. Anupam Swaminathan, Dr. Iqbal Hussain, Mr. Ronald Thomas, Dr. K. Phillips, Dr, M. Waugh, Dr, Chang**

1. SCOPE

Scope Analytics

***Agents*: System analysts, business analysts; agriculture scientists, engineers;**
***Moves* : Critical success factors analysis, Requirements management;**
***Security parameters*: define a set of sustainable development goals for poverty control.**

- **Food security : zero hunger;**
  - **Security against climate change, flood, drought, storm, cyclone, snowfall, rainfall, bushfire, attack of wild animals (e.g. elephants), paste;**
- **Home security : disaster proof nano-housing schema;**
  - **Security against earthquake, fire, flood, storm, cyclone, snowfall, rainfall, attack of wild animals and insects; act of terrorism, theft;**
- **Garments and consumer goods security;**
- **Responsible consumption and production through optimal resource planning and supply chain management;**

Prof. Boris Zekov and Dr. Chang are analyzing the above scope analytics in terms of food security, home security, garments and consumer goods security. The basic objectives are responsible consumption and production through optimal resource planning and supply chain management and emerging technologies on agriculture, housing, textiles and chemical engineering. Agricultural engineering is the engineering of agricultural production and processing through various disciplines (e.g. agriculture science, rural sociology, agriculture economics, mechanical, chemical, civil, electrical, food science); the basic objectives are to improve the agricultural productivity in terms of quantity and quality, efficacy and sustainability of agricultural practices. Agriculture is a set of specific activities

which transform the environment for the production of animals and plants for human use.

There is scope of innovation, adoption and diffusion of emerging technologies on agricultural science, plant breeding, genetics, plant pathology, horticulture, soil science, agronomy, agricultural biotechnology, fertilizer, entomology, production techniques, irrigation management, drought resistant crops and animals, development of new pesticides, yield sensing technologies, simulation models of crop growth, minimization of the effects of pests (e.g. weeds, insects, pathogens, nematodes) on crop or animal production systems, transformation of primary products into end consumer products, production, preservation, and packaging of dairy products, prevention and correction of adverse environmental effects, soil degradation, waste management, bioremediation and agricultural biotechnology (e.g. genetic engineering, molecular markers, molecular diagnostics, vaccines, tissue culture).

.

2. SYSTEM

System Analytics

***Agents*: system analysts, business analysts, scientists, engineers;**

***Objects / entities*: sustainable smart cities, smart villages,**

***Moves* : requirements engineering, system design, prototype testing, erection, installation, testing, commissioning;**

***Emerging technologies*: innovate a set of emerging technologies based on global security parameters and sustainable development goals.**

- **Food and beverage security**
    - **Smart farming through automation and infrastructure development in agricultural engineering;**
        - **Soil management (plough, hoe, cultivator**
        - **Seeding (seed drill for sowing of seeds)**
        - **Fertilizer / manures**
            - **organic manure (compost manure for organic firming)**
            - **inorganic manure (N, P, K, Ammonium Sulphate)**
        - **Irrigation (pulley, canal, bucket, Parsie wheels)**
        - **Weeds (e.g. grass, Partheneum, Amaranthus, Chenopodium) control using weedicide**
            - **inorganic control**
            - **organic control**
        - **Paste control for protection from the attacks of bacteria, fungi, virus and rats**
            - **inorganic control (DDT, BHC, Malatheon; salts of S, Cu, Zn, P)**
            - **organic control (using parasites and predators)**
        - **Harvesting (thrashing, winnowing, combine harvestor)**
        - **Storage / warehousing (silo)**
    - **Automation and civil infrastructure (e.g. warehouses) for animal husbandries (fisheries, dairy, poultry, epiculture, sericulture);**

    - Electrical (solar water pump);
    - Mechanical (solar power enabled tractors, net, trollers);
    - Biotechnology;
    - Genetic engineering;
    - Chemical (organic and inorganic fertilizer, pesticides);
    - Food processing technology
    - Digital technologies :
        - ERP-SCM system
            - Supply chain planning (demand, inventory, production capacity);
            - Supply chain collaboration
                - Collaborative planning, forecasting and replenishment (CPFR) system
                - Sourcing
            - Supply chain execution
                - Warehouse management system (WMS)
                - Transportation management system (TMS)
                - Pricing system
- ✪ Home security (disaster proof nano-housing schema, roof-top solar panels, civil, mechanical, metallurgical, virtual reality);
- ✪ Garments and consumer goods security : chemical (jacket, rain coats), textile, agriculture, process manufacturing, retail;

Dr, Kallis and Dr. Swaminathan are exploring the system associated with smart villages and smart cities. The key focus areas are solar water pump for agriculture and nano housing schema. They are analyzing the technology of solar water pumps. What is a solar pump and how is it different from conventional pumps? What are various types of solar water pump? What are the differences between surface and submersible pumps? Is a DC pump more efficient than AC pump? What are the advantages? What are the disadvantages such as impact of cloudy and foggy days and natural disaster? What are the basic working principles, irrigation capacity and average discharge? What is the procedure of site selection, erection, testing, and commissioning and relocation procedures of solar pump? What is the outcome of cost-benefit analysis? What are the marketing, promotion, advertising, sales and distribution strategies? What are the outcomes of technology life-cycle analysis?

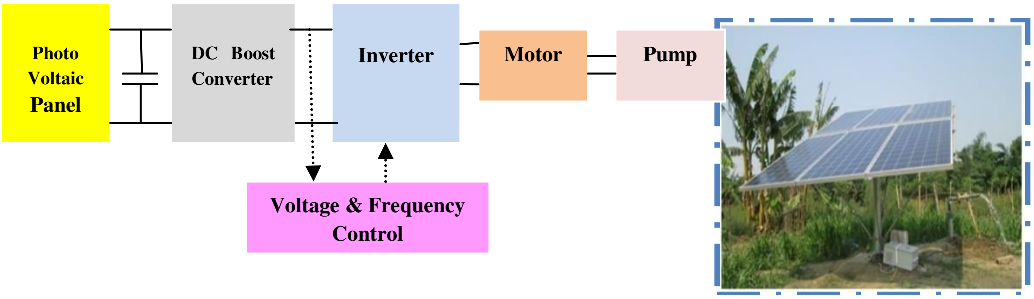


Figure 3.1: Solar water pump for agriculture

A solar water pump is a system powered by renewable solar energy [Figure 3.1]. It is used to extract water from various sources of water (e.g. lake, pond, river, borewell) for agriculture, irrigation and domestic drinking water applications (0.1-5 HP), municipal and rural community applications (15 - 100 litres of water per peak watt). For example, 2 HP and 7.5 HP pump may supply water to 2 and 10 acres of land respectively but this data may vary depending on the level of ground water and the type of irrigation required for a particular crop. A solar water pump can be used effectively for domestic application and irrigation (e.g. submersible, surface or deep well) in agriculture. It gets electrical power from solar array wherein a number of solar modules are connected in series or parallel. The array converts solar radiation into electrical energy which is controlled by a variable frequency driver and enables the connected pump to draw water from ponds, rivers or bore-wells and distribute the same to green fields directly for agriculture or to tanks for storage through pipeline. Solar power can be used as the energy supply of cold storage or warehouses which are generally used to store food grains, fruits and vegetables and can reduce the cost of storage and wastage of perishable items significantly.

A solar pump may be of different types such as AC/DC and submersible / surface pumps. A submersible pump is used in a borewell having water level deeper than 15 meters; a surface pump may be used in an open well, pond and water level less than 10 meter. The basic components of the system include solar panels, motor pump set, electronic controllers and inverters. Solar panels supply DC to the motor; AC pump requires an inverter to convert DC into AC. DC pumps may have higher efficiency over AC pumps and do not have inverter for operation. But, DC pumps may have constraints in terms of cost, repair and maintenance services. The discharge rate may vary 15-20 Litres of water per peak watt depending on solar intensity, location and seasonal factors.

Solar water pumps offer many advantages as compared to conventional nonrenewable energy driven pumps such as cost of fuel and maintenance, low voltage regulation, power cut and environmental pollution (e.g. air, water, soil) problems. It can be installed at remote areas; it has fewer moving parts and less chance of wear and tear; the system needs minimal maintenance like cleaning of the panels on a regular basis. It is easy to operate and do not require lubricants. But, the pump may not work effectively during cloudy and foggy days; it need to the conventional grid. Solar panels may be damaged due to hail storm, cyclones and direct lightning strike (if no lightning arrester is used). Solar panels should be installed in areas free of shade, dust and dirt; should be easily accessible for cleaning and should be as close as possible to the pump and water source. It is interesting to exercise a comparative analysis on the cost of AC and DC solar water pumps of various suppliers, subsidies and promotional efforts initiated by the state and central governments of various countries globally.

Solar microgrid for rural electrification: **Let us consider the application of solar power for rural electrification: how solar power can illuminate the life of poor rural people. The innovative business model of solar power can save energy cost of rural people in domestic applications and agriculture. The peasants and farmers can reduce the cost of energy used in water pumps for irrigation in agriculture. It can**

improve the productivity required for green revolution. A smart *microgrid* is an interesting option of rural electrification. It consists of solar panels, power condition unit (PCU), distribution box (DB), battery system and loads. Its size depends on the load estimation and the number of PV panels and rating of solar cells. The PV panels comprise of a set of solar cells connected in series or parallel; they convert solar radiation into electrical power; the power flows from PV panels to PCU or power inverter; PCU controls, regulates and directs the power to various loads (e.g. domestic load, water pumps in Greenfield). The surplus power generated in the daytime is stored in the battery bank and may be utilized after the sunset. The typical energy demand of a rural house is approximately 3 units. For a village of 100 houses, a 5 KW microgrid may be useful. It can generate annual energy of Rs. 50000. It is an approximate calculation.

2.2 Home Security - Nanohousing Technology

The expert panels are exploring the option of nanohousing technology to ensure home security. Nanohousing system is basically an innovative and sustainable architectural proposition based on green concept for residential use and pre-engineered structure made from cement fiberboard, recycled light gauge steel and polyurethane foam, creation of flexible spaces using suspending technology and use of renewable energy systems. This is an optimistic and environmental solution for the global housing issue of very small living spaces at affordable prices. Nanohouse may be suitable for a family of three in an area of 270 sq ft.; the suspending technology may be able to nearly double the size of the living area within this space by transforming common living space by day into two separate bedrooms by night.

2.3 Garments & consumer goods security

Textile manufacturing technology ensures garments security. Fibre is converted into yarn and yarn into fabric. These are then dyed or printed, fabricated into clothes. Different types of fibres are used to produce yarn. Cotton is the most important natural fibre; there is demand of other various types of products at fair and affordable price such as jackets, rain coats and sweaters. There is scope of automation at various stages of textile manufacturing: cultivating and harvesting, preparatory processes, spinning, cloth yarn, bundle, sewing thread, weaving, knitting, finishing, marketing, sales and distribution. There is scope of improvement of various processes at the spinning, fabric forming, finishing and coloring processes. There is scope of innovation and production of various types of consumer goods at economies of scale such as shoes, sandals, talc powder, soap, sanitizer, bodywash, facewash, perfume, saving cream and toothpaste through the advancement of chemical engineering, pharmacy and biotechnolgies.

3. STRUCTURE

Structure Analytics

***Agents*: System analysts, business analysts;**
***Moves*: Design and configure**

- **Organization structure**
    - **Technology forums**
    - **National level : Government, NGOs, research organizations, ;**
    - **International level : strategic alliance among global organizations ;**
    - **System architecture ; Innovate a set of emerging technologies as per the goals of food, home , garments and consumer goods security;**
    - ***Level 1*: information technology, electrical, electronics, chemical, mechanical and civil engineering;**
    - ***Level 2*: Identify fundamental building blocks of information technology**
        - **Computing schema**
        - **Data schema : database (demand, supply, production, distribution), big data analytics;**
        - **Networking schema : web connectivity;**
        - **security schema**
        - **application schema : SCM system**
            - **Supply chain planning (demand, inventory, production capacity);**
            - **Supply chain collaboration (CPFR, sourcing)**
            - **Supply chain execution (WMS, TMS, pricing system)**

Dr. Iqbal Hussain is analyzing the structure of emerging technologies of agriculture and nano-housing schema. He is presenting the basic architecture of nanohousing system. Nanotechnology offers various types of benefits such as optimization of existing objects, reduction in weight and volume, reduction in number of production stages, efficient use of materials, reduced need for maintenance, reduction in the consumption of raw materials and energy and reduced CO_2 emissions, conservation of resources, greater economy and comfort. It is an interesting option to explore how to use steel, concrete, hard materials and glass for nanohousing schema with economy of scale; how to ensure circulation of natural light; how to use concrete and stone innovatively and how to create a sense of comfort and beauty.

The best way to address issues of energy in nanohousing schema is to use solar power. A comfortable modern design of responsive architecture must explore that the nanohousing schema should generate its own energy and create a comfortable living environment continually adapting to changing weather conditions. Energy efficient infrastructure may be equipped with solar panels and sensitive lighting systems which minimizes CO_2 emissions and reduces total energy costs for the city and its inhabitants to reach zero emission. Nanohousing schema should use climate responsive design techniques such as sun shading, cross ventilation and direct evaporative cooling to reduce the need for air conditioning. Lotus effect is expected to reduces the cleaning requirement and maintenance demands.

4. SECURITY

Security Analytics

***Agents*: kids, children, youth, men, women, senior people;**
***Organization* : food security council of global organization, research organization;**
***Verification mechanism*: audit *security intelligence*.**

- ***system design policy*: verify rationality, fairness, correctness, transparency, accountability, trust and commitment;**
- ***system performance:* verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness, reachability, synchronization, safety (from natural disaster, war, bioterrorism, acts of terrorisms);**
- ***access control* in technology innovation: verify authentication, authorization, correct identification, privacy, audit confidentiality, data integrity and non-repudiation;**
- ***malicious attacks*: verify the risk of false data injection, shilling (push and pull) and fault injection attack;**
- ***corruption* in resource planning and supply chain management;**

call threat analytics and assess risks of emerging technologies on agriculture, animal husbandries, nanohousing, textile and chemical engineering.

- **what is corrupted or compromised (agents, design schema)?**
- **time: what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights: how and why did it occur? do cause-effect analysis on system performance, exception and alerts.**
- **recommend: what is the next best action?**
- **predict : what is the best or worst that can happen?**

***Output*: security intelligence**

Mr. Ronald Thomas is discussing the security of emerging technologies related to food, home, garments and consumer goods. It is essential to verify rationality, fairness and correctness of the design of the systems. It is also crucial to verify system performance in terms of reliability, consistency and safety. The systems should be developed by a set of authorized agents. It is also important to verify the risk of corruption in resource planning and supply chain management and various types of *malicious attacks*.

5. STRATEGY

Strategy Analytics

***Agents*: System analysts, business analysts, scientist, engineers, technology management consultants;**
***Strategic moves* : Focus on emerging agricultural, animal husbandries, civil, construction, architecture and textile technologies.**

- ✪ **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements – scope, system, structure, security, strategy, staff-resources, skill-style-support;**

- **Define a set of security goals and emerging technologies accordingly.**
- **Do SWOT analysis: strength, weakness, opportunities and threats of existing technologies as compared to emerging technologies;**
- **Fair and rational business model innovation**
  - **Who are the consumers?**
  - **What should be the offering of products and services?**
  - **What do the consumers' value?**
  - **What is the rational revenue stream ?**
  - **How to deliver values to the consumers at rational cost?**
- **Do technology life-cycle analysis on 'S' curve : presently at growth phase of 'S' curve.**
- **Explore technology innovation-adoption-diffusion strategy.**
  - **Smart farming**
  - **Automation in agriculture, animal husbandries, textile engineering**
  - **Collaborative planning, forecasting and production and distribution to minimize wastage;**
  - **Adoption of digital technologies such as ERP, SCM and WMS for storage, distribution and transportation;**
  - **Artificial rainfall and water conservation to tackle drought;**
  - **Safety from natural disasters, malicious attacks of fungi, bacteria, viruses and insects and acts of terrorism;**
  - **Environmental pollution control (e.g. air, water, soil);**
- **Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.**
- **Adopt '4E' approach for the development of underdeveloped zone by building smart villages and optimal resource planning, allocation and distribution : envision, explore, exercise and extend.**

Prof. Phillips and Dr, Waugh are exploring the strategies for the innovation, adoption and diffusion of emerging agriculture, nanohousing, textile and consumer goods technologies. The forums have explored a set of interesting strategic moves for the innovation, adoption and diffusion of emerging technologies in agriculture, animal husbandries, civil, construction, architecture and textile engineering. It is essential to innovate dominant design of intelligent machines and equipments at optimal cost. Most of the technologies are at emergence phase of S-curve (e.g. solar water pump, electrical and hybrid vehicles like tractors).

The digital technologies are at growth phase of S-curve. Commercial SCM, WMS and ERP systems are already available in COTS market. It is essential to customize these softwares as per the requirements of related sectors. It is a challenging task to develop web enabled information system to support collaborative planning, forecasting, production and distribution mechanism in agriculture. It is a hard challenge to protect the crops, food, beverage and perishable goods from natural disaster and malicious insects, viruses, bacterias and worms; these technologies are evolving with the advancement of chemical engineering, genetics and biotechnologies. Innovative strategies should be explored for conservation of water through artificial rainfall.

Dr. Waugh is exploring the strategy of organic farming, a sustainable agricultural practice based on natural ecological systems and biowastes. The other key areas are genetic engineering, biofertilization and smart sustainable agriculture. This practice avoids the use of synthetic pesticides and fertilizers; the basic objective is to sustain soil quality and health. Composting of organic residues and the use in agriculture bring back plant nutrients and organic matter to the soil; but there are risks of presence of heavy metals or organic pollutants. This strategy increases soil organic matter; enhances soil fauna and soil microbial biomass and stimulates enzyme activity leading to increased mineralization of organic matter, Na, K, P, C and improved resistance against pests and diseases.

Organic farming increases soil cation exchange capacity, improves soil structure, soil physical characteristics (e.g. aggregate stability, bulk density, porosity, available water capacity, and infiltration). But, Nitrogen mineralization takes place relatively slowly. Increased available water capacity may protect crops against drought stress. Global food crisis is coupled with the environmental impact of global warming and fuel shortages; transgenic methods may be required to enhance food production and quality. Widely used chemical insecticides (e.g. phosphine, methyl bromide) are losing their utilities due to insect resistance and environmental damage. Traditional plant breeding methods may be adopted for insect resistance. For example, transgenic Avidin, a protein naturally occurring in egg white is useful for the protection of rice, maize, potato and apple leaf from insect pests. Agriculture should be cost-effective and efficient. It is interesting to explore the scope of low cost moisture, temperature sensors for optimizing water usage and yield, and radar sensors for monitoring any invasion in the farm, smart water management and consistent monitoring for weather conditions.

6. STAFF-RESOURCES

Staff-resources Analytics

do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- ***Man* (human capital management [scientists, business analysts, system analysts, project managers, engineers, peasants, farmers, labourer], talent acquisition, talent retention, training, reward and recognition);**
- ***Machine* (tools, mechanical [tractors, machines], electrical [solar water pumps], computer hardware, software, internet), textile machines);**
- ***Material* (seed, fertilizer, paste controllers, crops, vegetables, fruits, food grains);**
- ***Method* (process innovation for resource allocation and distribution);**
- ***Money* (optimal fund allocation, project management, resource allocation, resource distribution, loan from bank, land management, insurance);**

Dr. Iqbal Hussain and Mr. Thomas are presenting staff-resources for the innovation of emerging technologies on agriculture, nanohousing, textile and

chemical engineering. Optimal planning and capacity utilization of various types of resources is essential for promoting best practice in agriculture and animal husbandries. The expert panel have identified five critical resources for green, blue and white revolution - man, machine, materials, method and money. The advancement in agricultural engineering should support process innovation in agriculture and animal husbandries. It is essential to train and educate the staff (e.g. peasants, farmers, labourers, scientists, engineers) on new technologies - how to operate intelligent automated machines, how to install solar water pump and solar microgrid, how to do maintenance and how to use materials (e.g. seeds, fertilizer, paste controllers) in cost effective ways. The most critical issue is management of financial resources for the innovation and promotion of new technologies. It is rational to use ERP system for optimal planning and capacity utilization of resources; it is an interesting option to explore ERP system for sales and distribution, materials management, HR management, financial and cost control for the innovation of emerging agricultural technologies.

7. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- ***Skill*: knowledge of operation and best practices of agriculture and animal husbandries, nanotechnology, civil, construction and architecture, textile engineering, technical, system administration, management, governance, supply chain management;**
- ***Style*: leadership, shared vision, goal setting, intelligent communication, risk assessment and mitigation, innovation project management;**
- ***Support* : proactive, preventive and reactive support.**

The expert panel are exploring skill-style-support for the innovation, adoption and diffusion of emerging agricultural, nano-housing, textile and consumer goods technologies. The panel have identified a set of key areas for skill development such as design of agricultural machinery, equipments and structures, agricultural resource management (e.g. land), water management, conservation and storage for crop irrigation and livestock production, surveying and land profiling, climatology and atmospheric science, soil management and conservation, soil erosion control, seeding, tillage, harvesting and processing of crops, livestock production (e.g. poultry, fish, dairy animals), waste management, (e.g. animal waste, agricultural residues and fertilizer runoff), food processing technology, electrical motors, physical and chemical properties of materials (e.g. fertilizers, paste controllers), crop processing and storage, controlled environment agriculture and experiments related to crop and animal production. Innovation leaders must have shared vision, goal, communication, project management, coordination skills and rational decision making capabilities. The technical staff should have capabilities on proactive and reactive support of automated machines, equipments, tools and systems.

It is essential to develop skills in various branches of engineering such as mechanical, electrical, civil, chemical, digital technology, genetics, biotechnology

and agricultural engineering;, domain knowledge of best practices and process innovation in agriculture, fisheries, poultry, dairy, poultry, epiculture and sericulture and related research and development. Agricultural engineers are expected to develop skills in planning, supervising and managing the building of irrigation, drainage, flood water control systems, environmental impact assessments, agricultural product processing, interpretation of research results and implementation of best practices. Generally, they work in academic institutes of agriculture engineering, government agencies, consulting in private engineering firms, manufacturing industries of agricultural machineries, equipments, processing technology and structures for housing livestock and storing crops and also in production, sales, management, research and development on applied science.

FURTHER READING

- **Alban C, Job D, Douce R (2000) Biotin metabolism in plants. Annu Rev Plant Physiol Plant MolBiol 51:17–47.**
- **http://nanolivingsystem.com**
- **Nayar, A., Puri, V.: Smart farming: IoT based smart sensors agriculture stick for live temperature and moisture monitoring using Arduino, cloud computing & solar technology. In: The International Conference on Communication and Computing Systems (ICCCS-2016).**
- **Food and agriculture organization of the United Nations.**
- **Wu, Q., Liang, Y., Li, Y., Liang, Y.: Research on intelligent acquisition of smart agricultural big data. In: 2017 25th International Conference on Geoinformatics, pp. 1–7. IEEE (2017).**
- **Wolters, S.L., Balafoutis, T., Fountas, S., van Evert, F.K.: D1.2 Research project results on Smart Farming Technology, Project coordinator: Spyros Fountas.**
- **Gondchawar, N., Kawitkar, R.S.: IoT based smart agriculture. Int. J. Adv. Res. Comput. Commun. Eng. (IJARCCE) 5(6), 177–181 (2016).**
- **Vidya Devi,V., MeenaKumari, G.:Real-time automation and monitoring system formodernized agriculture. Int. J. Rev. Res. Appl. Sci. Eng. (IJRRASE) 3(1), 7–12 (2013)**
- **Sen, S., Madhu, B.: Smart agriculture: a bliss to farmers. Int. J. Eng. Sci. Res. Technol. (2017)**
- **Alin S, Xueyuan L, Kanamori T, Arao T (1996) Effect of long-term application of compost on some chemical properties of wheat rhizosphere and non-rhizosphere soils. Pedosphere 6:355–363**
- **Amlinger F, Favoino E, Pollak M, Peyr S, Centemero M, Caima V (2004) Heavy metals and organic compounds from wastes used as organic fertilisers. Study on behalf of the European Commission, Directorate-General Environment, ENV.A.2**
- **Cook J, Keeling A, Bloxham P (1998) Effect of green waste compost on yield parameters in spring barley (Hordeum vulgare) v. Hart. Acta Hortic 469:283–286**

- **Cortellini L, Toderi G, Baldoni G, Nassisi A (1996) Effects on the content of organic matter, nitrogen, phosphorus and heavy metals in soil and plants after application of compost and sewage sludge. In: De Bertoldi M, Sequi P, Lemmes B, Papi T (eds) The science of composting. Blackie Academic & Professional, London, pp 457–467.**
- **Majeed, A (19 January 2009), Cotton and textiles - the challenges ahead ,Dawn-the Internet edition, retrieved12 February 2009**
- **"Machine processes" , Spinning the Web, Manchester City Council: Libraries, retrieved 29 January 2009**
- **"Cultivating and Harvesting" , Spinning the Web, Manchester City Council: Libraries, 2009**

Quiz

- **What is the scope of smart agriculture and nousing technologyfor smart city and smart villages?**
- **What is the dominant design of these technologies?**
- **What are the basic elements of the system architecture ?**
- **What do you mean by technology security? How can You verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis and SWOT analysis of these technologies?**
- **How to manage resources for innovation project of these technologies**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How do You manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**

SESSION 4: EDUCATION SECURITY - EMERGING TECHNOLOGIES, POLICY, METHODOLOGIES & MATERIALS

Event : Technology for humanity and global security summit ;
Venue: Education security hall, Technology park : Sanada;
Time Schedule : 2 p.m.. – 6 p.m. , 15.8.2020;
Agents : Representatives of various global organizations (nations, child, peace, health, bank, economic forum), Technology management experts from science and technology forums, engineers, scientists, educationists, representatives and ministers from the departments of education, human resources management, children, women and family welfare of developed, developing and underdeveloped countries, business development consultants from high technology, representatives from NGOs;
Topic of discussion and key focus areas: Education security, education methodologies, education technologies, education policy;
Keynote speakers : Prof. Diana Fisher, Dr. Thomas Merkle, Prof. S. Robinson, Prof. Dilip Kumar, Prof. T. Mandella, Dr. M. Khalid.

1. SCOPE

Scope Analytics

***Agents*: System analysts, business analysts, scientists, engineers;**
***Moves* : Critical success factors analysis, Requirements management;**
***Security parameters*: define a set of sustainable development goals to ensure education security in synchronization with other security parameters (financial security, social security, nutrition, garments, healthcare, energy, communication, logistics)**
***Application domains*: child education (pre-primary, primary, secondary, higher secondary), higher education (graduation, post graduation), adult education, continuity education, education for special children (e.g. learning disability, physically challenged, mentally challenged, depression, Dyslexia)**
***Objectives* : Skill development**

- **Quantitative and verbal skills, languages (mother tongue, foreign languages), common sense economics, general knowledge, decision making capabilities, analytical and logical reasoning, vocational skill;**
- **Sports and games (indoor and outdoor games, yoga, meditation);**
- **Extracurricular activities (debate, music, dance, general knowledge, event management, social works)**
- **Human values (morality, attitude, behavior)**
- **Creativity and innovation**

***Methodologies*:**

- **learning with fun**
- **simulated learning environment**
- **multi-dimensional education methodologies (written test, quiz, case discussion, story telling, role playing, project, research, assignments, consulting, experiment, practical lab works)**

Prof. Diana Fisher is presenting the scope of education security globally. Education is fundamental building block for achieving full human potential and promoting global development. Providing universal access to quality education is the key challenge to our society in terms of economic growth, social justice and equality, scientific advancement, national and global integration and cultural preservation. Universal high quality education is the best way forward for developing and maximizing rich talents and resources for the good of the individual, the society, the country and the world. Our ability to provide high quality educational opportunities to the young community will determine the future of our world. The global education development agenda is to ensure inclusive and equitable quality education and promote life-long learning opportunities for all. Such a challenging goal demands fundamental rethinking and radical redesign of global education system. It is important to solve a set of critical fundamental problems to implement global education policy effectively?

- **What is the *scope* of global education policy: What is the goal and shared vision?**
    - **Education for all : discriminately or non-discriminately?**
    - **Education is a life-long learning process (child education, adult education, continuity education, education for special children).**
    - **Contribute, contribute, contribute: apply knowledge rationally, analytically, logically with positive attitude.**
    - **Reduce the weight and load of schoolbags anyway by how or by cook!**
- **What is the design of to-be flexible education *system*? What are the gaps, loopholes and open points of as-is education system?**
- **What is the *structure* of future education system and the regulator for effective creation, storage, transfer and application of knowledge?**
- **How to ensure and verify the *security* intelligence of future education system?**
- **What is the *strategy* of knowledge management in education policy? What is the strategic roadmap to implement a rational education policy? How to explore collective intelligence, collaborative intelligence, machine intelligence, business intelligence (i.e. corporatization / commercialization of education) and security intelligence concurrently?**
- **What are the criteria of *staff-resources* fit for the education policy: man, machine, material, method (i.e. process innovation) and money (fund)? What are the optimal mix of education methodologies, right education materials and fund allocation protocols?**
- **What are the *skills, style* (TQM: Total Quality Management) and *support* essential to implement the education policy? What should be the right education technology?**

2. SYSTEM

System Analytics

***Agents*: System analysts, business analysts, technology management consultants, scientists, engineers;**
***Moves* : requirements engineering, system design, coding, prototype testing, erection, installation, testing, commissioning;**
***Emerging technologies*: Innovate a set of emerging technologies based on education security (digital technology, information technology, electrical, electronics, telecommunication, chemical, mechanical, civil);**

- **Electronics and telecommunication (smart phones, mobile phones, smart boards, projectors, Internet, digital library, e-books, printer, xerox machine, phones, fax, projectors); Digital technology (computer, tablets);**
- **Electrical (power system, solar power at academic institutions, solar microgrid)**
- **Mechanical (furniture, pipeline, Physics lab, geometry box, engineering drawing tools [scale, T], engineering lab);**
- **Chemical (chemistry lab, paper, pen, pencil, rubber, cutting tool, bag, shoe, socks, shirt, trousers, whitener, paint color, color pencils);**
- **Bio science lab (botany lab, zoology lab, human physiology lab, genetics lab, biotechnology lab, biomedical lab);**
- **Civil (building, road, gym, playground, car parking space);**
- **Metallurgy (steel structure, glass, wood, aluminum. tin)**
- **Technology for multi-dimensional education methodology (practical lab works, projects, case discussion, consulting assignments, research assignments, written test, quiz, supervised and unsupervised learning to avoid rot learning, vocational training for skill development)**

Dr. Thomas Merkle, Prof. S. Robinson and Prof. Dilip Kumar are presenting the essential features of future education system. The human society is undergoing rapid changes in the knowledge landscape with advances in applied arts, science and technologies. The evolution of technologies for humanity, business analytics, data science, soft computing, AI, law, security, management, medical and social sciences is redefining the skill of global workforce and job profile with multidisciplinary abilities.The learners must not only learn but more importantly learn how to learn effectively. The traditional obsolete dead methods of rote learning must be rejected. The future generation education system is expected to reduce mental stress and information overloading and should promote intelligent learning mechanisms: how to think critically and solve problems rationally, how to be creative, innovative and multidisciplinary, how to innovate, adapt and absorb new technologies ans how to gain satisfactory and value adding job opportunities.. The education system is expected to be experimental through intelligent laboratory activities, holistic, integrated, inquiry driven, discovery oriented, learner centred, interactive discussion based, flexible and interesting. It is a challenging task to grow interests among the learning communities through innovative education methodologies and materials. The education system should also promote culture, ethics and moral values through extracurricular activities such as sports and games, yoga, meditation, music, dance, debate, applied arts and crafts. The education system

must be associated with logical, analytical, rational, intelligent and caring academic community.

3. STRUCTURE

Structure Analytics
***Agents*: System analysts, business analysts;**
***Moves*: Design and configure**

- **Organization structure**
    - **Education forums**
    - **National level**
        - **Government, NGOs, research organizations,**
        - **ministries of education and human resources (school education, higher education);**
        - **Regulator having a *cellular structure* having different cells (science, engineering & technology, management science, medical science, law, arts)**
    - **International level : strategic alliance among global organizations;**
- **System architecture ; Innovate a set of emerging technologies as per the goals of education security;**
    - ***Level 1*: information technology, electrical, electronics, chemical, mechanical and civil engineering;**
    - ***Level 2*: Identify fundamental building blocks of information technology (computing schema, data schema [e-books, digital library], networking schema (internet), security schema, application schema [software])**

Dr. M. Khalid is trying to explore the gap between the current state of learning outcomes and what is required in future. It is essential to adopt a set of major reforms that can incorporate quality, equity and integrity into the education system, including preprimary, primary, sencondary, higher secondary and higher education system. In many developing countries, the structure of higher education system is illdefined, corrupted, compromised and also neglected. It is not a easy tasl to offer quality education for all learners regardless of their social and economic background. For example, if courses such as technology management and technologies for humanity are not taught at the technical institutes properly, the effects will be inevitable; the technologies will be selected irrationally by hype and rumour. Is the future education policy too much focused on the hype of digital technologies (e.g. online learning) and neglecting other streams (e.g. Physics, Chemistry, Biology, Lab works), education methodologies and technologies? Why the education system is so lagging in the underdeveloped and developing world?

4. SECURITY

Security Analytics
***Agents*: kids, children, youth, men, women;**

***Verification mechanism*: call threat analytics and assess risks of emerging education technologies.**

- **what is corrupted or compromised (agents, computing schema, communication schema, data schema, application schema)?**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights : how and why did it occur? do cause-effect analysis on performance, sensitivity, trends, exception and alerts.**
- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**
- **what are the strength, weakness, opportunities and threats of online and offline education technologies?**

audit *security intelligence*.

- **audit authentication, authorization, correct identification, privacy, confidentiality, data integrity and nonrepudiation of education policy makers;**
- **verify rationality, fairness, correctness, transparency, accountability, trust and commitment of the education policy in human capital development;**
- ***system performance:* verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness and safety of education technologies; ensure safety of the learners from war, bioterrorism, migration and natural disaster;**
- **assess the risk of *multi-party corruption* in education system *(*politics, ragging, free riding, discrimination, hate crimes, malpractice, dishonesty, ethics);**
- **verify the risk of false data injection, shilling (push and pull), denial of service (DoS) and fault injection attack on education system.**

The basic objective of the expert panel is to revise and revamp various aspects of the education structure, regulation and governance to create a new education system that is aligned with the sustainable development goal of the summit. Prof. T. Mandella is analyzing the security of future education system. Education must develop not only cognitive capacities (basic capacities of literacy and numeracy) and higher order cognitive capacities (critical thinking and problem solving) but also social, ethical, and emotional capacities of the learners. It is crucial to develop faculties as the most respected and essential members of our society by ensuring livelihood, respect, dignity, autonomy, quality control, accountability, trust and commitment. It is a challenging task to provide quality education to all students with focus on historically marginalized, disadvantaged, and underrepresented groups. Education is a great leveler and is the best tool for achieving economic and social mobility, inclusion and equality, local and global needs of human society, rich diversity and culture, social, cultural and technological needs, ethics, self-confidence, self-knowledge, cooperation, and integration.

5. STRATEGY

Strategy Analytics

***Agents*: educationists, system analysts, business analysts, scientist, engineers;**
***Strategic moves* :**

- **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements (scope, system, structure, security, strategy, staff-resources, skill-style-support);**
- **Define a set of security goals and emerging technologies accordingly.**
- **Do SWOT analysis: strength, weakness, opportunities and threats of existing offline technologies as compared to emerging online technologies;**
- **Fair and rational business model innovation for education sector**
  - **Who are the consumers?**
  - **What should be the offering of products and services?**
  - **What do the consumers value?**
  - **What is the rational revenue stream?**
  - **How to deliver values to the consumers at rational cost?**
- **Do technology life-cycle analysis on 'S' curve: presently at growth phase of 'S' curve.**
- **Explore technology innovation-adoption-diffusion strategy.**
- **Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.**
- **Adopt '4E' approach for the development of underdeveloped zone by building smart villages and optimal resource planning, allocation and distribution (envision, explore, exercise, extend).**

The expert panel have explored a set of interesting strategic moves for the innovation, adoption and diffusion of emerging technologies in education sector. The education policy is expected to be defined based on fundamental rethinking and radical redesign of as-is education system globally, identification of gaps and design of to-be system rationally. It may not be an intelligent approach to copy online education system blindly in the present environment of global economic shock and advancement and threats of emergent technologies (e.g. communication; 1G->2G->3G->4G->5G->6G->7G->8G->9G->10G...., high risk of obsolescence of phone sets, generation of e-wastes). The education policy should be based on an optimal mix of supervised and unsupervised learning mechanisms which should promote creativity, innovation, self-confidence and skill development through motivation, commitment, trust and fair rational efforts of the academic community. It is also required to explore the scope of other learning mechanisms such as transfer, batch, online and dropout learning.

The education policy is too much focused on time period of various academic programmes; there should be more focus on other critical success factors such as total quality management, education methodology, education technology and education materials. The to-be education policy should explore the scope, system, structure, security, strategy, staff-resources, skill, style, support, shared vision and the ultimate goals of education system in terms of fairness, correctness, transparency, accountability and rationality. The change of time period from 3 to 4 years for graduation or (5+3+3+4) school education system should not be a time

pass; the time should be properly utilized through real contributions of the academic community for the development of the nation and human society globally.

In many countries, the student community exert maximum effort, time and cost on account of pre-primary and school education and preparation for aptitude tests and become exhausted physically and mentally to create real path breaking contributions in the domain of higher education at colleges, universities and branded academic institutes. There is less focus and fund allocation on higher education system, innovation, research and development; so the number of contributions, ideas and innovation is less in the domain of higher education. Another important issue is complexity: there is less focus on real contributions in science, engineering and technologies as compared to applied arts and entertainment since it is hard to innovate in science (mathematics, physics, chemistry, biology, engineering, medical and management) as compared to create stories (e.g. statistical juggleries, emotional false data injection attack, emotional blackmail, luxurious thoughts) in other domains based on common sense. The academic community and top talent are too busy in exploring simple schemes of various luxurious event management programmes and corporate communication; less focused on complex brain storming sessions as compared to the education system in developed countries.

The concept of single regulator is interesting but what should be the structure of single regulator? Single regulator should have a *cellular structure* having different cells: science, engineering & technology, management science, medical science, law, arts etc. If there is no proper regulatory control, the education system may collapse in the coming future. The regulatory body is expected to ensure corporate social responsibilities of various academic institutions and academic programmes. Absolute independence often creates pockets of inefficiencies, corruption and lack of commitment in as-is education system at various academic institutions. Benchmarking, standardization and total quality control is essential for talent management, reward, recognition, placement and job assistance. Why so many seats are vacant in technical institutes each year? There is sufficient infrastructure but the capacity utilization factor is very poor. Why?

The design of to-be education system should be structured, compact and free from malicious attacks (e.g. ragging, free riding, mental stress, depression, information overloading). Each course should be modernized and clearly outline the objectives, motivation, pedagogy, evaluation methodology, bibliography etc. The evaluation methodology should be multi-dimensional (e.g. Quiz and written test: 30%, case discussion: 20%, project: 30%, consulting assignment: 10%, research: 10%). What are the strength and weakness of open book examinations? The sole focus on online quiz contest based on MCQ may result a dull education system in future. In school education, (5+3+3+4) system may be interesting but the students should do their assignments and projects independently otherwise activity based learning may become totally vague. Which is preferred: activity based learning or (skill + value) based learning? If the activities or problems are solved by the parents or tutors of the students solely, the learners may not be able to develop problem solving skills in real-life. Multiple choices are interesting in selection of courses but the learners need focus and depth of knowledge to become experts. There may be the risk of loss

of focus. The books should be compact and written intelligently with no overlap, vague data content and information overloading. Special children (e.g. Dyslexia) need different education system. Use of mother tongue or local language is important but the options of foreign languages (e.g English) are also necessary. Focus on conceptual learning, problem solving, creativity and innovation, practical experiments, lab works and skill development are interesting options. *Simulated virtual lab* may be cost effective but may affect the learners in science, medical, engineering and technology streams. Virtual lab should be used with physical labs concurrently. The education policy should protect the learners from only 'writing, writing, reading; reading, reading, writing, typing, typing, typing' and various types of healthcare problems of eye, ear and mind due to excessive use of mobile phones and tablets!

Benchmarking, standardization, joint ventures and strategic alliance with foreign institutes in innovation, research and development (e.g. Ph.d., Postgraduate) may be an interesting option to improve the quality of education. Absolute independence of academic institutes may result corruption and inefficiencies in many pockets such as admission, education methodology, technology, innovation and knowledge management.

Vague topics of projects and research for Ph.d., Postgraduate and Graduate programmes are often selected by the academic community randomly as per personal whims and fancies; complex topics are often avoided and simple topics are chosen to complete research by how or by cook within deadline; the topics should be selected based on the needs of the country, society, industry and the world. The research programmes are expected to be well-defined, well-organized, structured, properly planned; the hardness and complexity of research problems should be challenged honestly. The ultimate objectives should be to create contributions for path breaking innovations. Existing research programme gives too much focus to course work and comprehensive qualifying examinations of the researchers; they should devote and dedicate more time to their thesis works and actual research contributions. They should be able to work sincerely with a free mind, free flow of information, collaboration and resources. Most surprisingly, in as-is system, they spend more time in event management and composition of stories; less time in actual innovation. That is why, the underdeveloped and developing countries are lagging so much in creativity and innovation as compared to the West. There should be a balanced approach; some researchers are totally indifferent to publication of research papers; some others are workaholic to large number of publications, some others are busy in knowledge manipulation but the ultimate outcome may be garbage input garbage output (GIGO). Many research guides may be really experts but less committed; some others may have lack of knowledge and no interest; some may be egoists. The researchers are expected to be guided properly; this is an issue of style of leadership, goal setting and intelligent vision of the system administrators, faculties and research guides.

Is it practically feasible to design academic curriculum: Certificate after 1 year, Diploma after 2 years, Degree after 3 years and Honours after 4 years? Many academic programmes are crippled with dead, obsolete courses having no depth and breadth; modern and advanced complex topics are avoided; quality research

publications are not included even in graduation levels; such types of programmes need complete overhauling. Availability of right resources (e.g. books, journals, software, hardware) at right time and correct use of the same is very important.

Another important issue is peculiar testing and evaluation system. Online test security is a critical concern today. Is the online testing system (e.g. quiz contest) really evaluating the performance of the students correctly in higher education (e.g. engineering, medical, management, science, law)? Is the online test free from various malicious attacks by the adversaries in India today : session hijack, hanged web portal of academic institutions, networking problem of mobile service provider, privacy, confidentiality, internet traffic congestion, link failure, Denial of Service (DoS) attack, power cut (load shedding), delay, mobile charging problem, battery charging problem, internet access problem, sybil attack, natural disasters (e.g. cyclone, rainfall, storm), data integrity, non-repudiation, authentication, authorization, correct identification, trust, commitment, fairness, correctness, transparency, accountability, corruption, reliability, consistency, resiliency etc. The students are forced to just uploading and downloading files into or from whatsapp or ticking options on the portal; there is no test of depth and breadth of knowledge through such so called quiz contest. There is no logic and rationality of the decision making authorities of independent academic institutions; the standards and quality of higher education system may be becoming a vague silly joke and the present situation of epidemic is adding fuel to the fire. There is no value given to innovation, knowledge and skill development of the young student community.

Law of average having no head or tail is a critical threat. Many boards, councils and academic institutions may be in a hurry with a casual approach in testing and evaluation - how to publish final results by how or by cook; poor performances may be getting maximized; good performers may be getting victimized. There may be no rationality in heuristics of evaluation system. This is just like the film 'Heerak rajar deshe' directed by the great Satyajit Roy : 'Janar kono sesh nai; janar chesta britha tai'; (There is no end of knowledge; so, it is useless to learn anything); as if marks are bribed to the students in the name of peculiar rules and regulations. What may be the solution to this problem: is it 'dari dhare maro tan, raja hobe khan khan'! [Renew system and governance]. It is essential for the governments of various countries to rescue the education system from sureshot collapse, disaster and uncertainty in the coming future through an intelligent, rational unbiased national education policy.

6. STAFF-RESOURCES

Staff-resources Analytics

do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- ***Man*** **(human capital management [learners, faculties, system administrators, scientists, business analysts, system analysts, project managers, engineers], talent acquisition, talent retention, training, reward and recognition)**
- ***Machine*** **(tools, computer hardware, software, internet, mobile phones, tablets)**

- ***Material*** **(book, notebook, paper, pen, pencil, rubber, color, geometry box, bag)**
- ***Method*** **(process innovation for resource allocation, education methodology)**
- ***Money*** **(optimal fund allocation, project management, resource allocation, resource distribution, education loan from bank)**

Optimal planning and capacity utilization of various types of resources is essential for promoting best practices and quality management in education sector The expert panel have identified five critical resources for re-engineering in education sector : man, machine, materials, method and money. The critical issue is management of financial resources for the innovation and promotion of new technologies. It is rational to use ERP system for optimal planning and capacity utilization of resources; it is an interesting option to explore ERP system for efficient resource management. .

7. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- **Skill (knowledge of operation and best practices of education sector, engineering, technical, system administration, management, governance, supply chain management);**
- **Style (leadership, shared vision, goal setting, intelligent communication, risk assessment and mitigation, innovation project management);**
- **Support (proactive, preventive and reactive support)**

The expert panel have identified a set of key areas for skill development such as knowledge of operation and best practices of education sector, engineering, technical, system administration, management, governance and supply chain management. Innovation leaders must have shared vision, goal, communication, project management and coordination skills and rational decision making capabilities. The technical staff should have capabilities on proactive and reactive support of equipments, tools and systems. It is essential to develop skills in various branches of engineering such as mechanical, electrical, civil, chemical,, digital technology, domain knowledge of best practices and process innovation in education sector and related research and development. With the support of digital technologies, it is possible to develop a sophisticated knowledge management system (e.g. digital libraries, e-books, e-journals, e-papers,e-magazines). But, how many learners are really motivated to understand the distributed education materials during various academic programmes (e.g. engineering, medical); it is an issue of trust and commitment and real challenge to the education world. There should be proper integration among education technology, policy and methodology during today's age of technology transition.

Quiz

- **What is the scope of smart education technology?**

- **What is the dominant design of these technologies?**
- **What are the basic elements of the system architecture?**
- **What do you mean by technology security? How can You verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis and SWOT analysis of online and offline technologies?**
- **How to manage resources for innovation project of these technologies**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How do You manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**

Further Reading

- **Kusumita Chakraborty. 2005. A study of literacy achievement in literacy centres of West Bengal. Registration Number : 306 Ph.D. (Education). Department of Education, Calcutta University, India.**
- **Aronowitz, S. (1994). Technology and the future of work. In G. Bender & T. Druckrey (Eds.), *Culture on the brink: Ideaologies of technology* (pp. 15–30). Seattle: Bay Press.**
- **Ballengee-Morris, C., & Stuhr, P. L. (2001). Multicultural art and visual cultural education in a changing world. *Art Education, 54*(4), 6–13.**
- **Barbosa, A. M. (1991). Art education and environment. *Journal of Multicultural and Cross-Cultural Research in ArtEducation, 9*(1), 59–64.**
- **Freedman, K. (1995). Educational change within structures of history, culture, and discourse. In R.W. Neperud (Ed.),*Context, content, and community in art education*. New York: Teachers College Press.**
- **Lanier, V. (1969). The teaching of art as social revolution. *Phi Delta Kappan, 50*(6), 314–319.**
- **Morley, D. (1992). *Television, audiences, and cultural studies*. London: Routledge.**
- **Neperud, R. (1973). Art education: Towards an environmental aesthetic. *Art Education, 26*(3).**
- **Rose, G. (2001). *Visual methodologies*. London: Sage.**
- ***Multicultural and Cross-cultural Research in Art Education, 14*, 80–91.**
- **Solso, R. (1997). *Mind and brain sciences in the 21st century.* Cambridge, MA: MIT Press.**
- **Tavin, K. (2000). Just doing it: Towards a critical thinking of visual culture. In D. Wiel & H. K. Anderson (Eds.). *Perspectives in critical theory: Essays by teachers in theory and practice* (pp. 187–210). New York: Peter Lang.**

SESSION 5: HEALTH SECURITY - CANCER CARE, BIOMEDICAL TECHNOLOGY and ARTIFICIAL IMMUNE SYSTEM for EPIDEMIC CONTROL

***Event* : Technology for humanity and global security summit**
***Venue*: Health security hall, Technology park: Sanada**
***Time* Schedule : 2 p.m.. – 6 p.m., 16.8.2020**
***Agents* : Representatives of various global organizations (Health, Economic forum), Technology management experts from science and technology forums, Social engineers, Social scientists, representatives and ministers from the departments of child, women and family welfare of developed, developing and underdeveloped countries, CEOs of life science corporations, business development consultants of life science, pharmaceuticals.**
Topic of discussion and key focus areas : Health security, cancer care, biomedical technologies, Artificial immune system, Epidemic and pandemic control

Keynote speakers : Prof. Bob Taylor, Dr, Jim Morrison, Prof. Michel Bolton, Prof. P. Kar, Prof. David Nissim, Dr. Arvind Gurumurthy, Dr. Muller, Dr. Nil Harvey

1. SCOPE

Scope Analytics

***Agents*: System analysts, business analysts; scientists, doctors, engineers;**
***Moves* : Critical success factors analysis, Requirements management;**
***Security parameters*: define a set of sustainable development goals on healthcare security, cancercare**
Application domains:

- ***Cancer :* cancer of mind / psycho-oncology, neural control and coordination, chemical coordination and integration, digestive system, respiratory system, cardiovascular system, excretory system, locomotion and movement system, reproductive system;**
- **Biomedical technology innovation : artificial pancreas, artificial liver, artificial kidney, artificial limbs, artificial cardiovascular devices, oral insulin;**
- **Artificial immune system for epidemic control.**

Prof. P. Kar is starting the session based on key focus areas such as *c*ancer prevention, proactive approach, reactive approach, bad luck, deep learning, optimal margin classifier, support vector machine, precision medicine, regenerative medicine, integrated medicine, cancer genomics, CNN, intelligent reasoning, bio-medical technology, oral insulin, artificial pancreas, artificial kidney, artificial liver, artificial cardiovascular devices, artificial limbs, laser, surgical robotics, wearable computing, concurrent engineering, technology innovation, epidemic control,

pandemic outbreak, Intelligent broadcast, online grievance management system, articial immune mechanism, self-nonself classification, danger signal, clonal selection, hotspot, cluster, social distancing, security intelligence, business intelligence, bio-terrorism, life science supply chain, and healthcare service chain.

This session explores an emerging technology for prediction and prevention of cancer.. The complexity of emerging technology has been analyzed in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support. Presently, the technology of cancer care is passing through the growth phase of S-Curve. The technology has been analyzed in terms of a set of intelligent strategic moves such as proactive and reactive approach, deep learning, optimal margin classifier, intelligent reasoning and biomedical instrumentation. Intelligent reasoning has been explored in terms of case based reasoning, perception and common sense. It is also essential to adopt a set of effective reactive strategies such as genomics, precision, integrated, regenerative and alternative medicines to fight against cancer. We have presented a deep analytics based cancer prevention mechanism (DACPM) balancing proactive and reactive approaches. The mechanism defines human biological system from the perspectives of application, computing, networking, data and security schema. This work also analyzes different types of cancer through DACPM.

This session also shows the application of deep analytics '7-S' model on the innovation of bio-medical technology for cancer care. The complexity of biomedical technology has been analyzed in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support. The scope of biomedical technology has been explored in terms of artificial pancreas, artificial liver, artificial kidney, artificial cardiovascular system and artificial limbs. The critical observation is that oral insulin is a rational, simple, practically feasible and safe option as compared to artificial pancreas. It is hard to develop artificial kidney, liver and pancreas which can mimic all the functions of related biological organs. The concept of oral insulin is now at emergence phase of technology life-cycle; artificial cardiovascular devices and limbs. It is rational to adopt proactive and reactive approaches to overcome the constraints of biomedical technology. This work also explores the scope of laser therapy, pervasive and wearable computing and surgical robotics for cancer care. Is it possible to innovate an affordable cheap test kit for cancer care which should be able to detect cancer of human beings by measuring a set of critical health parameters (e.g. blood, urine, sweat, stool, saliva, mucosa, semen etc.) through biosensors in an automated manner? Can AI promote such complex innovations in future?

This session also presents the construction of a deep analytics based cancer prevention mechanism (DACPM) balancing proactive and reactive approaches. It defines human biological system from the perspectives of application, computing, networking, data and security schema of an information system. The strategic moves of DACPM include deep learning, intelligent reasoning, threat analytics, optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan and adaptive secure multi-party computation. The performance of human biological system is expected to be verified through the properties of adaptive secure multiparty computation: fairness, correctness,

accountability, transparency, rationality, trust, commitment; authentication, authorization, correct identification, privacy, audit; safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency, robustness and stability of application integration. It analyzes the complexity of the mechanism in terms of computational cost of deep learning algorithm. This work is specifically focused on reasoning nine test cases through DACPM in depth to fight against the epidemic of cancer: The human biological system is assumed to be a computer. It is not a rational thinking that the most of the causes of cancer are due to bad luck; it is still not known enough about the causes and prevention measures of cancer. Deep analytics does not necessarily mean deep learning algorithm, it is also associated with intelligent reasoning – analytical, logical, common sense, case based reasoning and also perception to fight against the epidemic of cancer. A human agent must have common sense healthcare knowledge base for proper biological system control through intelligent self-assessment, self-confidence, life-style, diet control and right decision making at right time. It demands the necessity of learning the basic concept of reasoning and common sense healthcare through an effective knowledge management system based on deep analytics and intelligent broadcast communication.

The basic objective of this session is to generate a rational cancer prevention plan subject to financial constraints. The work has reviewed the relevant literature on cancer, oncology and deep learning and has adopted analogical reasoning as research methodology.

Technological innovations are practical implementation of creative novel ideas into new biomedical devices. Many potential ideas pass through the wide end of an innovation funnel but very few may become successful, profitable, economically and technically feasible products in future. It is an interesting research agenda whether deep analytics may be an effective tool for the diffusion of biomedical technology in future. It is a multi-dimensional analysis wherein seven factors must be integrated, coordinated and synchronized. This session shows the application of deep analytics '7-S' model on innovation of bio-medical technology.

Recently, there is a trend of cross fertilization between five disciplines: medical science, management information system, artificial intelligence, artificial neural network and management science. This work is associated with the problem of cancer prevention. Cancer is a costly, global and complex problem; it results a major obstacle to human development and well-being. The attack of cancer has increased from 12.7 million (2008) to 14.1 million (2012) and this trend is projected to continue about 25 million cases over next two decades; the greatest impact will be in low and middle income ill equipped countries. The future of a cancer patient depends on the living zone. In less economically developed countries, cancer is diagnosed at more advanced stages while access to effective treatment is limited or unavailable. The highest-income countries often struggle with the spiraling costs of cancer treatment and care. Cancer has a social cost, human potential is lost and cancer care has an escalating economic impact. It is essential to identify the causes and prevention strategies for cancer control.

Let us first look at bio-statistics of cancer. It is a major cause of morbidity and mortality, with about 14 million new cases and 8 million deaths in 2012, affecting

populations in all countries and all regions. Among men, five most common sites of cancer were lung (16.7%), prostate (15.0%), colorectum (10.0%), stomach (8.5%), and liver (7.5%). Among women, five most common sites of cancer were breast (25.2%), colorectum (9.2%), lung (8.7%), cervix (7.9%), and stomach (4.8%). There were 8.7 million people (older than 15 years) alive with cancer diagnosed in the previous year, 22.0 million in the previous 3 years, and 32.6 million in previous 5 years. The worldwide estimate for the number of cancers diagnosed in childhood (ages 0–14 years) in 2012 is 165000 (95000 in boys and 70000 in girls). The highest incidence rates are associated with high income countries of North America and western Europe, Japan, Korea, Australia, and New Zealand. More than 60% of cases and 70% of deaths occur in Africa, Asia, and Central and South America. Cancers are caused by mutations that may be inherited or caused by environmental factors or DNA replication errors.

Dr. Kar has defined the structure of human biological system from the perspectives of application, computing, networking, data and security schema of an information system. The application schema is related to the function and features of a specific biological system. The networking schema is related to the configuration of the system such as nodes and interconnections among the nodes. The computing schema deals with the protocol, process, procedure and mechanisms of a system and its various components. The data schema is associated with various entities, their attributes and interrelationships, inputs and output of a system. The security schema verifies the disorders of the system and protects the system through various means such as vaccination precision, regenerative and integrated medicine, chemotherapy and laser.

In this session, the scope of cancer has been explored in terms of (i) cancer of mind, (ii) neural control and coordination : brain cancer, (iii) chemical coordination and integration : breast cancer (iv) digestion and absorption : liver, pancreas, stomach and colorectal cancer (v) respiratory : lung cancer, (vi) body fluids circulation : blood cancer, (vii) excretory : renal cancer and urinary bladder cancer, (viii) locomotion and movement: bone cancer and (ix) reproductive system : ovarian and testis cancer.

Dr, Rina Brown and Prof. Bob Taylor have explored the scope of emerging biomedical technologies in terms of artificial pancreas vs. oral insulin, artificial kidney, artificial liver, artificial cardiovascular devices (e.g. heart valves, stents, pace makers, artficial limbs, arms, legs and laser therapy. The scope of innovation on biomedical technology should be explored rationally through intelligent analysis of the basic objectives, goals, needs, constraints and mechanisms; strength, weakness, opportunities and threats of various strategic options. First, it is essential to understand the mechanisms of various human organs (e.g. pancreas, liver, kidney, heart, limb, brain) in terms of human physiology, input, output, feedback control, function, process, chemical reaction, secretion of enzymes and hormones, coordination, integration and system performance. Next, it is rational to analyze whether it is practically feasible to make artificial organs which can mimic various functions of biological organs of human body in the best possible ways. The scope of biomedical technology spans over several domains such as artificial pancreas, liver, kidney, cardiovascular system and limbs

***Artificial pancreas*: Let us first do scope analysis on oral insulin vs. artificial pancreas for the treatment of diabetes; which is more feasible technology innovation and why? Pancreas synthesizes insulin which extracts glucose from carbohydrate for the supply of energy and storage. It controls blood sugar level and prevents hyperglycemia or hypoglycemia. Insulin is a collection of 51 amino acids with two chains A (21 amino acid) and chain B (30 amino acid) linked by disulfide bridges. Diabetes is a chronic disease, it arises when sufficient amount of insulin is not produced by the pancreas (Type 1 diabetes) or insulin which is formed is not utilized properly by the body (Type 2 diabetes). It leads to an elevation of blood glucose level (hyperglycemia). Diabetes is the most common endocrine disorder. It is a real challenge to find out effective administration and delivery mechanism of Insulin. Subcutaneous (SC) route may lead to hyperinsulinemia. Repeated injections if insulin may result various types of health problems such as lipoatrophy or lipohypertrophy, peripheral hyperinsulinemia, peripheral hypertension, atherosclerosis, cancer, hypoglycaemia and other adverse metabolic effects. Can an artificial pancreas mimic all the functions of a biological pancreas? It is essential to explore alternative route such as oral insulin which mimics the typical insulin pathway within the body after endogenous secretion subject to various constraint such as good bowel absorption and very low oral bioavailability of insulin.**

***Artificial liver* : Next, let us consider the scope analysis of artificial liver. Liver is a complex organ doing various vital functions such as synthesis, detoxification and regulation; its failure may result a life threatening condition. Liver failure (LF) can either occur as acute liver failure (ALF) due to intoxication or as acute-on-chronic liver failure (AoCLF). The common symptoms are icterus, hepatic encephalopathy and impairment of coagulation and may result even multi organ failure. In case of liver failure, water-soluble toxins (e.g. ammonia) and albumin-bound toxins (e.g. bilirubin, amino and fatty acids) may accumulate and cause encephalopathy and dysfunction of other organs. Detoxification and regulation can be addressed by artificial devices similar to dialysis, the synthetic function of the liver can only be provided by living cells. We have done analysis on strength, weakness, threats and opportunities of artificial liver and have also outlined a liver protection mechanism by adopting an optimal mix of proactive and reactive approaches.**

***Artificial kidney*: Next, let us consider the innovation of artificial kidney. There are various therapies of kidney problems [e.g. end-stage renal disease (ESRD, continuous renal-replacement therapy (CRRT)] which cause sepsis, systemic inflammatory response syndrome, acute respiratory distress syndrome, congestive heart failure, tumorlysis syndrome and genetic metabolic disturbances. The dominant therapies are hemodialysis and hemofiltration. An artificial kidney should perform three physical processes efficiently that determine the removal rate for uremic toxins through membrane-based devices: c*onvection* removes toxin through a semipermeable membrane; d*iffusion removes* smaller molecules with high diffusion coefficients and a*dsorption*.**

***Artificial cardiovascular devices*: Next, let us consider the technological innovation of artificial cardiovascular devices. Cardiovascular disease (CVD) is the leading cause of death worldwide. In this domain, the technological innovation is facing several challenges such as improved device function (e.g. cardiac valves, stents, pacemakers**

and defibrillators, vascular grafts, hemodialyzers, catheters, circulatory support devices and blood oxygenators), complex and challenging cardiovascular surgical procedures (e.g. open- heart surgery), medical therapies (e.g. dialysis), valve replacement problems (e.g. thromboembolism, hemolysis, paravalvular regurgitation, endocarditis and structural failure of the valve); artificial heart valves design (e.g. percutaneous or minimally invasive valve implantation and tissue engineering), progress in stent technology to reduce restenosis and improvement of stent outcome, development of pacemakers, cardioverter-defibrillator (AICD), cardiac electrophysiologic devices from the perspectives of improved device function, dual chamber activity, advances in technology and implantation techniques, development of artificial lung for acute cardiopulmonary bypass and improved biocompatibility.

***Artificial limbs*: The basic objective of prosthetics research is to design and develop artificial arms, hands and legs which can be used flexibly with physiological speeds-of response and strength and controlled almost without thought. The current state is basically a tool rather than a true limb replacement. The prosthesis is an interchangeable device that is worn and used as needed and then ignored. The major constraints of prostheses are weight, power, size and sufficient number of appropriate control sources to control the requisite number of degrees of freedom. The system requires better sensors, actuators and multifunctional control mechanisms. The basic building blocks of artificial limbs are mechatronics and robotics; current prosthetic components and interface techniques are still a long way from realizing the aforesaid objectives.**

Dr. Muller is exploring the scope of various types of epidemic and pandemic outbreak and is suggesting a set of intelligent strategic moves as countermeasures. It is rational to adopt an efficient system; an optimal mix of e-governance (e.g. online grievance management system), broadcast communication protocol and artificial immune mechanism to fight against natural disaster, epidemic and pandemic outbreak. It is essential to analyzes security, strategy, staff-resources and skill-style-support for efficient coordination and collaboration in corporate governance. There is threat of bio-terrorism on the soft targets (e.g. life-science supply chain and healthcare service chain). Is the conflict between security intelligence and business intelligence inevitable?

Epidemic and pandemic is a critical causal factor of poverty of human society globally. Can emerging technologies be used to fight against such calamities effectively? Dr. Muller is xploring the scope of epidemic and pandemic outbreak in depth; *Pandemic* is more dangerous than *epidemic*. When an epidemic spreads globally, it is called pandemic. In case of epidemic, a disease spreads at very fast rate witin a particular period among one or more communities. For example, WHO has recently declared the outbreak of novel Corona virus as Pandemic, but it is controllable. There are other various types of threats of epidemic globally due to environmental pollution such as air, water, soil, light and sound pollution. The issues have been already discussed during session 2.

Epidemic may happen due to *air pollution* like dust at construction sites and industrial plants; smoke from vehicles; paste control problem (e.g. mosquitoes,

flies), malnutrition in slum areas, improper cleaning of garbages and stool of street animals? Epidemic may occur due to *water pollution* in supply of dirty drinking tap water caused by leakage in pipelines, contamination and jerms in water storage system, malfunctioning of tube wells, water filtering problem, mixing of water from drainage system and tap water pipeline, unprotected selling of unhealthy food (e.g. oily spicy biriyani) and beverages at retail outlets and by hawkers being contaminated by flies; risks of diahorrea, stomach upset and loose motion. Epidemic due to *soil pollution* and earthquake caused by random digging of soil for construction projects, erosion of soil at riverbeds; jamming in drains due to plastics, improper cleaning of drainage and sewage system; There is threat of epidemic due to *light pollution* in slum areas, unplanned urban development planning, blockage of sufficient sunlight into residential areas (e.g. houses, flats, multi-storied buildings) Epidemic due to *sound pollution* may be caused by playing loud and wild music, fireworks, activities at construction sites and industrial belts.

3. SYSTEM

System Analytics

***Agents*: Doctors, scientists, system analysts, business analysts, engineers;**

***Moves* : requirements engineering, system design, prototype testing, installation, testing, commissioning;**

***Emerging technologies*: innovate a set of emerging technologies based on health security parameters and sustainable development goals.**

- **Cancer prevention**
  - ✪ **Proactive approach**
  - ✪ **Reactive approach**
  - ✪ **Deep learning /* multi-model ensembling method */**
    - ▪ **Raw data collection**
    - ▪ **Data filtering**
    - ▪ **Feature selection**
    - ▪ **Cross validation**
    - ▪ **Configure deep learning architecture**
    - ▪ **Define training strategy(algorithm, learning rate, stopping criteria);**
    - ▪ **Call 1st stage classification algorithm**
    - ▪ **Call 2nd stage ensemble method**
    - ▪ **Testing strategy KDD**
  - ✪ **Intelligent reasoning**
    - ▪ **Case based reasoning**
    - ▪ **Perception common sense reasoning**
  - ✪ **Regenerative medicine**
  - ✪ **Precision medicine**
  - ✪ **Cancer genomics**
- ***Biomedical technology*: artificial pancreas, artificial liver, artificial kidney, artificial limbs, artificial cardiovascular devices, oral insulin;**
- ***Artificial immune system* for epidemic and pandemic control.**

Dr, Jim Morrison and Prof. Michel Bolton are presenting on emerging healthcare systems. Artificial intelligence (AI) is basically simulation of human intelligence. An intelligent reasoning system demands new data structure beyond knowledge base with envision, perception and proper assessment of a problem; reasoning is not effective when done in isolation from its significance in terms of the needs and interests of an agent with respect to the wider world. A rational reasoning system needs the support of an intelligent analytics. The basic objective is to evaluate the natural and adaptive immunity of a complex system. The evaluation of the immunity of a system involves modeling, defining complete specifications and verification.

First, it is essential to model the human biological system by proper representation of its various states and programs. Next, it is important to specify the properties of the system through logical reasoning. Finally, it is essential to develop a verification mechanism which justifies: does the model satisfy the properties indicating a healthy immune system? The evaluation of immunity of a system can be done by exhaustive search of the state space (local, global, initial and goal states and state transition relations) of a system through simulation, testing, deductive reasoning and model checking based on intelligent search. The procedure terminates with positive or negative answer; the positive answer indicates a healthy immune system; the negative results provide an error trace indicating incorrect modeling or specification of the system or the occurrence of malicious threats.

The human immune system is an adaptive, robust, complex and distributed information processing system which protects the health of the biological system from the attacks of malicious foreign pathogens (e.g. virus, bacteria, fungi, protozoa, parasitic worms). It discriminates the self from non-self elements. The immunity is either innate or adaptive; innate immunity detects and kills specific known invading organisms; adaptive immunity responds to previously unknown foreign organisms. AI community needs a new outlook, imagination and dreams to solve a complex problem like prevention of cancer through a set of simple mechanisms. There are some types of cancer due to bad luck. But, we still do not know enough about the causes and preventive measures of different types of cancer. The following section highlights two branches of artificial intelligence: (a) deep learning and (b) case based reasoning.

Deep Learning **: Cancer is a complex global health problem involving abnormal cell growth and a major cause of morbidity and mortality. It is challenging to predict cancer using machine learning algorithms based on gene expression or image data for effective and accurate decision making, diagnosis and detection at early stage. It is basically a classification problem which predicts and distinguishes cancer patients from healthy persons. Recently, deep learning has been explored in terms of ensemble approach that combines multiple machine learning models. It is an interesting strategic option to apply various classification algorithms on informative gene expression and then a deep learning approach is employed to ensemble the outputs of the classifiers. This deep learning based multi-model ensemble method is an accurate and effective method for cancer prediction as compared to single**

classifier. One of the critical issues is that it is irrational to mix data of various types of cancer and then apply deep learning based multi-model ensemble method on this mixed data. Rather, it is correct to apply deep learning algorithm on data set of different types of cancer separately such as lung, stomach and breast cancer.

Let us exercise SWOT analysis on deep learning. Deep learning is an efficient biomedical research tool in many potential applications such as drug discovery and biomarker development. A neural network may have a single hidden layer where DNN has many hierarchical layers of nonlinear information processing units. A simple neural network does not deal well with raw data whereas deep learning can be largely unsupervised and can learn intricate patterns from even high-dimensional raw data with little guidance. Only a deep circuit can perform exponentially complex computational tasks without requiring an infinite number of nodes. DNNs can process very large high dimensional, sparse, noisy data sets with nonlinear relationships. DNNs have high generalization ability; once trained on a data set, they can be applied to other new data sets; this is a requirement for binding and interpretation of heterogeneous multiplatform data. DNNs can be classified into networks for unsupervised learning, networks for supervised learning and hybrid or semi-supervised networks.

But there are some limitations such as black box problem in quality control and interpretation of high dimensional data; selection problem in choosing appropriate DNN architecture, high computational cost of time consuming training method, overfitting problem and the need for large training data sets that may not be readily available. In case of overfitting, training error is low but the test error is high.

***Training strategy* : Data analysis on gene expression level is one of the research hotspots today. There are various types of machine learning algorithm such as *k* - nearest-neighbor (kNN), support vector machines (SVM), decision trees (DT), random forests (RF), and gradient boosting decision trees (GBDT). But, each machine learning method has its own flaws in terms of classification accuracy and other performance measures. It is hard for SVM to find out an appropriate kernel function. DTs have over fitting problems and RFs require more samples to attain high classification accuracy. Each machine learning algorithm may outperform others; it is rational to adopt multiple learning algorithms for better performance. There are various types of ensemble methods such as bagging, boosting, linear regression, stacking, majority voting algorithm and deep learning. Majority voting considers linear relationships among classifiers.**

Deep learning has the ability to learn the intricate nonlinear structures from the original large data sets automatically. Deep neural networks can ensemble multiple classification models to predict cancer more accurately. To avoid over fitting, it is required to preprocess the raw data and employ differential gene expression analysis to select important and informative genes, which are fed to various classification models. A deep neural network is used to ensemble the outputs of multiple classification models to obtain the final prediction result. Deep learning based multi-model ensemble method makes more effective use of the information of the limited cancer data and generates more accurate prediction than single classifiers or majority voting algorithm. There are several open issues. Is it rational

to ensemble the outputs of multiple classification models to obtain the final prediction result for same type of cancer across different demographic profile of cancer patients or various zones of the world? Is it possible to ensemble the outputs of multiple classifiers for different types of cancer?

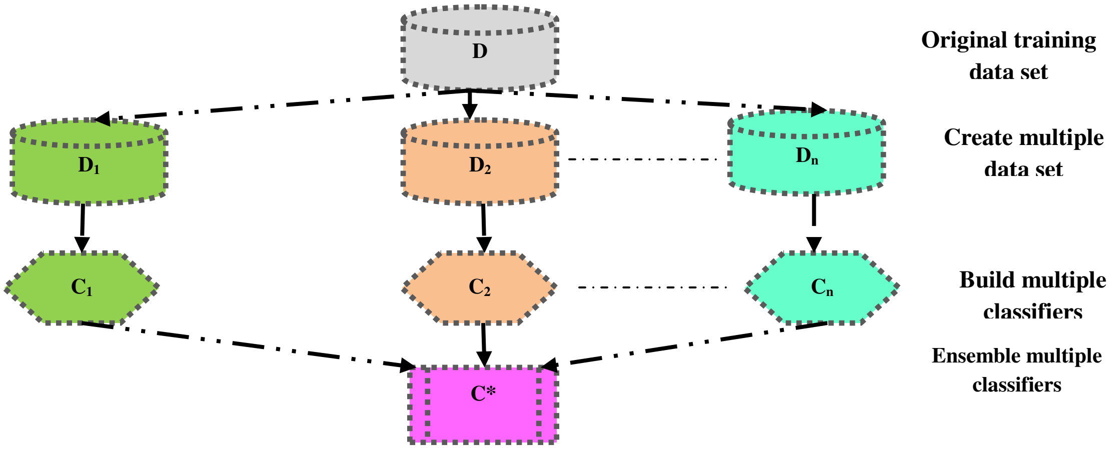

D
Original training data set
D1
D2
Dn
Create multiple data set
C1
C2
Cn
Build multiple classifiers
Ensemble multiple classifiers
C*

Figure 5.1. Ensemble learning method

Another critical issue is to improve classification accuracy in case of imbalanced, multi-class learning problems. Let us consider the case of bowel cancer data where a large number of examples of normal cases may exist with a much smaller number of positive cases of cancer. This data imbalance complicates the learning process and may result misclassification for the classes with fewer representative examples. Such uneven distribution may create a difficult learning process for finding unbiased decision boundaries. A regularized ensemble model of deep learning employs regularization that accommodates multiclass data sets, automatically determines error bound and penalizes the classifier when it misclassifies examples that were correctly classified in the previous learning phase and can attain superior performance in terms of improvement of overall accuracy for all classes.
Testing strategy: Let us consider three data sets of three kinds of cancers such as Lung cancer (LCD), Stomach cancer (SCD) and Breast cancer data (BCD).

- **ROC curve for LCD : True positive rate vs. false positive rate for KNN, SVM, DT,RF, Majority voting, ensemble**
- **ROC curve for SCD data**
- **ROC curve for BCDA data**
- **Dataset, data size, precision (%), recall (%), accuracy(%), CPU time(S)**
- **Predictive accuracy (%) of various classification algorithms**

Optimal Margin Classifier for Cancer Detection : The expert panel are trying to explore whether an efficient optimal margin classifier such as support vector machine can be applicable for detection of cancer. Here, the most important issue is the performance of SVM in terms of classification accuracy and privacy of data. Classification comprises of two subtasks: learning a classifier from training data

with class labels and predicting the class labels for unlabeled data using the learned classifier. Data can be stored as feature vectors. In the classification problem of detecting cancer, the training data comprises of patients with labels cancer or no cancer. Support Vector Machine (SVM) is the most well-known kernelized maximum margin classifier. The learning methodology is the approach of using examples to synthesis programs for computing the desired output from a set of inputs; it generates target decision function in hypothesis space. The learning algorithm selects training data as input and selects a hypothesis from the hypothesis space. There are various methods of learning such as supervised learning from training examples, unsupervised learning, batch learning and online learning. The next issue is generalization - how to assess the quality of an online learning algorithm? Consistent hypothesis performs correct classification of the training data. The ability of a learning machine to correctly classify data not existing in the training set is known as generalization. How to improve generalization: Ockham's Razor suggests that unnecessary complications are not helpful; it may result overfit.

Support Vector Machine (SVM) is a learning system that uses a hypothesis space of linear functions in a high dimensional feature space, trained with a learning algorithm from optimization theory that implements a learning bias derived from statistical learning theory. In case of pattern classification problem, the objective of SVM is to devise a computationally efficient way of learning for finding out an optimal capacity of the pattern classifier to minimize the expected generalization error on a given amount of training data by maximizing the margin between training patterns and class boundary. The basic properties of SVM are that the learning system is suitable for both linear and nonlinear problems, computationally efficient algorithm through modular and dual representation in Kernel induced high dimensional feature space and optimized generalization bounds.

Learning in Kernel induced feature space is as follows:

Target Function – $f(m_1,m_2,r) = C*m_1*m_2/r^2$; $g(x,y,z) = \ln f(m_1,m_2,r) = \ln C + \ln m_1 + \ln m_2 -2 \ln r = c+x+y-2z$; A linear machine can learn g but not f. A kernel is a function K such that for all $x,z \varepsilon X$;$K(x,z) = <\varphi(x). \varphi(z)>$ where φ is a mapping from input space X to inner product feature space F.

$<x.z>^2 = (\Sigma^n{}_{i=1} x_i z_i)^2 = (\Sigma^n{}_{i=1} x_i z_i) (\Sigma^n{}_{j=1} x_j z_j) = \Sigma^n{}_{i=1} \Sigma^n{}_{j=1} x_i z_i x_j z_j = \Sigma^{n,n}{}_{i,j=(1,1)} (x_i x_j) (z_j z_i) = \varphi(x). \varphi(z)$

Let us consider linear classification problem. Given a linearly separable training sample $S = ((x_1, y_1), \ldots.., (x_l , y_l))$, the hyperplane (w,b) realizes the maximal margin hyperplane with geometric margin $\gamma = 1/ \|w\|_2$ by solving the optimization problem : Minimize <w.w> Subject to $y_i (<w. x_i> + b) \geq 1$ where i = 1,....,l; In case of SVM, the strategy is to find the maximal margin hyperplane in kernel induced feature space. In case of linear classification problem, the equation of hyperplane is $f(x) = <w.x> +b = 0$ or, $f(x) = \sum^l{}_{i=1} w_i x_i +b = 0$; An input $x = (x_{1,....,} x_n)$ belongs to positive class if $f(x) \geq 0$; An input $x = (x_{1,....,} x_n)$ belongs to negative class if $f(x) < 0$. The decision function: $h(x) = \text{sgn} (f(x)) = \text{sgn}(<w.x> +b)$; Functional margin of an example (x_i, y_i) is $\gamma_i = y_i (<w.x_i> + b)$. Geometric margin measures the Euclidean distance between an example and the hyperplane, it is expressed as normalized linear function $(w/ \|w\|, b/ \|w\|)$. Updation rule of SVM algorithm in primal form is as follows: if γ_i or $y_i (<w.x_i> + b) \leq 0$ then $w_{k+1} \leftarrow w_k + \eta y_i x_i$, $k \leftarrow k+1$ $\gamma_i>0$ indicates

correct classification of the training example. Duality is the one of the basic features of Support Vector Machine; SVMs can be modelled as linear learning machines in a dual fashion. In this case, updation rule of the perceptron algorithm is expressed in dual form. The solution i.e. final hypothesis of weight vector is a linear combination of training points. Each pattern x_i is associated with an embedding strength α_i , which is proportional to the no. of times misclassification of x_i causes updation of the weight.

$w = \sum^{l}_{i=1} \alpha_i y_i x_i$

$f(x) = <w.x> +b = 0$

$= (<\sum^{l}_{i=1} \alpha_i y_i x_i.x> +b)$

$= (\sum^{l}_{i=1} \alpha_i y_i <x_i.x> +b)$

In the dual form, the updation rule and decision function can be expressed in the form of inner product space $<x_i.x>$.

Kernel Based Algorithms; Two separate learning functions; Learning Algorithm in an embedded space; Kernel function performs the embedding; Embed data to a different space; Possibly higher dimension; Linearly separable in the new space. Kernels themselves can be constructed in a modular way. Modularity is one of the important properties of SVM.

Learning In Kernel Induced Feature Space : Kernel methods exploit information about the inner products between data items. Kernel function can simplify the computation of separating hyperplane without explicitly carrying out the map in the feature space. The number of operations to compute the inner product space is not proportional to the number of features. Hence, high dimension of feature space does not affect the computation. Since F is high dimensional, the RHS of this equation is computationally very expensive.

$f(x) = <w.x> +b = (\sum^{l}_{i=1} \alpha_i y_i <x_i.x> +b)$; it is the equation of hyperplane in input space. $f(x) = <w. \phi(x)> +b = (\sum^{l}_{i=1} \alpha_i y_i <\phi(x_i). \phi(x)> + b)$; it is the equation of hyperplane in feature space where ϕ is a mapping from input space to inner product feature space. $f(x) = \sum^{l}_{i=1} \alpha_i y_i K (x_i.x) + b$ where K = Kernel function

Next, let us consider computation of geometric margin. Geometric margin is the functional margin of a normalized weight vector. In case of linear classifier, the hyperplane function (w,b) does not change if we rescale the hyperplane (mw,mb) where $m \in R^+$ due to inherent degree of freedom. So, to optimize the geometric margin, we can consider functional margin of 1 for two points x^+ and x^- . $<w.x^+> +b = +1$; $<w.x^-> +b = -1$; Geometric margin $\gamma = ½(\|w\|_2)$ $[(<w.x^+> +b) – (<w.x^-> +b)] =1/ \|w\|_2$.

SVM problem formulation is as follows. Given a linearly separable training sample $S = ((x_1, y_1), ..., (x_l, y_l))$, the hyperplane (w,b) realizes the maximal margin hyperplane with geometric margin $\gamma = 1/ \|w\|_2$ by solving the optimization problem - minimize <w.w> subject to $y_i (<w. x_i> + b) \geq 1$ where i = 1,....,l; this is a convex optimization problem minimizing a quadratic function under linear inequality constraints.

Primal Form ---- $L(w, b,\alpha) = 1/2<w.w> - \sum^{l}_{i=1} \alpha_i [y_i (<w.x_i> + b) - 1]$; SVM problem formulation is as follows.

$\partial L(w, b,\alpha)/\partial w = w - \sum^{l}_{i=1} \alpha_i y_i x_i = 0$; $\partial L(w, b,\alpha)/\partial b = \sum^{l}_{i=1} \alpha_i y_i = 0$; $w = \sum^{l}_{i=1} \alpha_i y_i x_i$

Dual Form ----- $L(w, b,\alpha) = 1/2<w.w> - \sum^{l}_{i=1} \alpha_i [y_i (<w.x_i> + b) - 1] = \sum^{l}_{i=1} \alpha_i - 1/2 \sum^{l}_{i=1} \alpha_i\alpha_j y_i y_j< x_i x_j>$

The quadratic form of SVM problem formulation is as follows. Given a linearly separable training sample $S = ((x_1, y_1), ..., (x_l, y_l))$, the hyperplane (w,b) realizes the maximal margin hyperplane with geometric margin $\gamma = 1/ ||w||_2$ by solving the optimization problem in dual form

Maximize $\sum^{l}_{i=1} \alpha_i - 1/2 \sum^{l}_{i=1} \alpha_i\alpha_j y_i y_j< x_i x_j>$

Subject to $\sum^{l}_{i=1} \alpha_i y_i = 0; \alpha_i \geq 0$

$w^* = \sum^{l}_{i=1} \alpha^*_i y_i x_i$ = Desired solution; $b^* = ½ [\max_{y_i = -1}< w^*.x_i > + \min_{y_i = 1}< w^*.x_i >]$

Optimal hyperplane --- $f(x,\alpha^*,b^*) = \sum^{l}_{i=1} \alpha^*_i y_i <x_i.x > + b^*$

The advantages of SVM is no local minima due to convexity of the quadratic optimization problem, it is an advantage over neural networks. The open issue is speeding up the training method, choice of appropriate Kernel functions and use of Kernel methods in other algorithms.

Case based reasoning (CBR) is a methodology for solving problems by utilizing previous experience. It involves retaining a memory of previous healthcare problems and their solutions and solving new problems by referencing the past cases. A healthcare expert (e.g. oncologist) presents a new query case to CBR system. The system searches its memory of past cases stored in case base and attempts to find a case that has the same problem specification of the current case. If the system does not find an identical case in its case base, it will attempt to find the case or cases that match most closely to the current query case. There are two different types of search such as similarity search and neighborhood search. In case of similarity search, the solution of the retrieved case is directly used for the current problem. The system adapts the retrieved cases if the retrieved case is not identical to the current case. In a complex search, the system requires the access of multiple case bases which are located at various locations. Let us consider a simple CBR algorithm.

CBR Mechanism

Agents: Healthcare consultant (e.g. oncologist);

Input: New case or query (q) regarding the immunity problem a patient;

Protocol:

Retrieve the most similar cases $(c_1,\ldots,c_k)$, k nearest neighbors w.r.t. q from the case base;

Adapt the proposed solutions to a solution s(q), compute s(q) by combining the solutions s_j of the cases c_j. s_j is weighted as per the differences between c_j and q;

Learn after applying s(q) to q in reality; Store the new solution in the case base for solving q'.

Evaluate performance: Rejection ratio = no. of unanswered queries / total no. of queries.

Output: Recommended solution;

CBR is selected for cancer due to various reasons. The healthcare domain has an underlying model, the process is not random and the factors leading to the success

or failure of a solution can be captured in a structured way. Cases recur in healthcare domain though there may be exceptions and novel cases. Healthcare solutions can be improved through case retrieval and case adaptation. Relevant healthcare cases are available at different healthcare institutes; it is possible to obtain right data. *Case retrieval* is the process of finding within the case base those cases that are the closest to the current case. There must be criteria that determine how a case is evaluated to be appropriate for retrieval and a mechanism to control how the case base is searched. Most often, an entire case is searched. But, partial search is also possible if no full case exists.

***A case* is a record of a previous experience or problem in terms of problem definition, patient's symptoms, drugs, solution methodology, test results and recommendations. A case base also stores global best practices, standards, valid drugs, price and contacts of specialists. Data is stored based on domain knowledge and objectives of the reasoning system. The cases should be stored in a structured way to facilitate the retrieval of appropriate case when queried. It can be a flat or hierarchical structure. *Case indexing* assign indices to the cases for retrieval and comparisons. There are different approaches of case retrieval. In case of nearest neighbor search, the case retrieved is chosen when the weighted sum of the features that match the query case is greater than the other cases in the case base. A case that matches the query case on n number of features is retrieved rather than a case which matches on k number of features where k < n; different features may be assigned with different weights. Inductive approach is driven by a reduced search space and requires reduced search time. This results reduced search time for the queries. Knowledge based approaches select an optimal set of features of case by using domain knowledge. The complexity of case retrieval depends on multiple factors: (a) number of cases to be searched, (b) domain knowledge, (c) estimation of the weights for different features and (d) case indexing strategy.**

***Case adaptation* is the process of translating the retrieved solution appropriate for the current problem; it adds intelligence to the recommendation process. There are various approaches of case adaptation. The retrieved case can be directly used as a solution to the current problem without any modification. Otherwise, the retrieved solution should be modified according to the current problem. The steps or processes of the previous solution can be reused or modified. The solution of the current case can be derived by combining knowledge of multiple retrieved cases. Case adaptation is a complex decision making task, it considers multiple factors: how close is the retrieved case to the query case? How many parameters are different between the retrieved and the query case? DMAs can apply common sense or a set of rules or heuristics for case adaptation.**

Making sense of the information found during an investigational web search is a complex task of case based reasoning. *Sense making* is to find meaning in a situation; it is the cognitive act of understanding information. The system should support collaborative information search by providing several rich and interactive views of the search activities of a group. One of the problems is the design of computer interfaces to enable sense making of the processed information. Sense making is not only important for individuals, but also for groups to achieve shared goals. Traditional sense making tools focus on data mining, provide better

information representation, visualization and organization of search results. But, it is also required to support the collaboration and communication that occurs among the investigators when they make sense of information together.

Dr, Jim Morrison and Dr. Arvind Gurumurthy are presenting on biomedical system for health security. It is essential to analyze in terms of state, complexity, feedback loop, physical and information flows. The basic objectives of system analytics are to analyze complex and dynamic interactions among various components of different types of biomedical devices such as artificial pancreas, liver, kidney, cardiovascular devices and limbs.

Artificial pancreas **: An artificial pancreas is expected to perform various types of functions such as continuous blood glucose monitoring without manual intervention of the user, monitoring trends of rising and falling blood sugars for the prediction of blood glucose levels in the immediate future, comparing blood sugar levels against a high threshold, and prompting for a correction bolus from the insulin pump and also comparing blood sugar levels against a low threshold and prompting to reduce the basal insulin from the pump. A stream of real-time data is used for close loop control of the insulin pump. The critical components of artificial pancreas are sensors, control algorithm and insulin pump.**

Artificial liver: **Next, let us consider the innovation of artificial liver. Liver failure can be overcome by orthotropic liver transplantation and this motivates the development of various artificial and bioartificial liver support devices [33-35, 36]. Artificial systems are based on the principles of adsorption and filtration; bioartificial devices are based on the provision of liver cells. Such artificial livers support detoxification, synthetic and regulative functions. In case of orthotropic liver transplantation, many patients may not survive until a suitable donor organ is available since donor organs are rare. Contraindications do not permit liver transplantation. For these problems, artificial devices are essential to bridge the patient to transplantation or temporarily support the failing organ. Cell free artificial systems use adsorption and filtration through removal of toxins from the patient's plasma. Haemodialysis is used for treatment of liver failure to remove water soluble toxins.**

A bioartificial liver device (BAL) is an artificial supportive device based on bioengineering for acute liver failure patient. Is it really feasible to develop a complex artificial liver which can mimic each function of normal and healthy liver? Dr. Kenneth Matsumara developed BAL based on liver cells obtained from an animal; a semipermeable membrane allows toxins and blood proteins to pass. Advancements in bioengineering techniques have led to improved membranes and hepatocyte from various cell sources such as primary porcine hepatocytes, primary human hepatocytes, human hepatoblastoma (C3A), immortalized human cell lines and stem cells. But, BAL can not replace liver functions permanently and serve as a supportive device for acute liver failure.

There are several limitations of bioartificial liver support. In most cases, the liver cells are separated from the patient's blood or plasma by at least one membrane which provides an immunological barrier limits the exchange of substances and reduces the effectiveness of the system. The blood/plasma flow is limited to 100–300

mL/min whereas the blood flow in a normal human liver is about 1500 mL/min. Then, what should be rational risk mitigation strategies for the problems of liver?
In charcoal haemoperfusion, there is risk of biocompatibility, loss of thrombocytes and clotting problems. Plasma exchange using filters requires a large plasma stock and bears the risk of infections. But, improved biochemical and clinical conditions and removal of toxins may not ensure survival benefit for the patients. It is essential to explore more sophisticated detoxification systems like albumin dialysis, fractionated plasma separation, continuous albumin purification system (CAPS) and Single Pass Albumin Dialysis (SPAD). Bioartificial systems give support in synthetic and regulatory function of the liver besides detoxifying the patient's plasma. Primary human cells meet the demand of biocompatibility. But, there is risk of infections and metastasis formation; the metabolic compatibility is not assured. It is really hard to find ideal cell source.

Artificial kidney **: Let us now consider the technological innovation of artificial kidney. The system needs focus on several areas such as maturation of hemodialysis and hemofiltration therapy, improvements in materials and hemodynamic areas, biocompatible materials, superior transport methods for toxin removal, bioartificial renal tubule, homeostatic functions, selective toxin removal without concomitant elimination of beneficial proteins, absorption removal pathway (with affinity methods to eliminate uremic toxins), tissue engineering and improved patient management techniques [18-24]. An artificial kidney is expected to perform a number of important metabolic, endocrine and active transport functions of living kidney.**

Artificial cardiovascular devices: **The basic objectives and challenges of the design of artificial cardiovascular devices is to replace various lost functions of heart, improve the performance of artificial valves, stents and pacemakers and to minimize the side effects and risks of complex surgical procedures. The number of surgical operations of valve replacement, stents and pacemakers has been increasing day-by-day due to various reasons like congenital valve defects and acquired valve disease of various patient groups and valve location. Valve replacement can be done for aortic or mitral valves. The design of artificial valves is evolving based on minimally invasive valve implantation and valvular tissue engineering through the advancement of computational fluid dynamics and computationally intensive simulation modeling techniques. Simulations can predict the performance of both bioprosthetic and mechanical valves and analysis of various complications such as structural failure, thromboembolism, hemolysis, paravalvular regurgitation and endocarditis.**

Stent is used to hold tissue in place or provide a support for a graft and applicable to the diseases of peripheral and coronary arteries. Stents may be of two types such as balloon-expandable and self-expanding. The design of stent is evolving in terms of advanced material science [metal, alloys (e.g. tantalum, steel, Nitinol), biodegradable and nondegradable polymeric stents], improvement of system performance, reduction of the risks of restenosis, ease of handling and stable long term system performance, simple and effective deployment method. Percutaneous Transluminal Coronary Angioplasty (PTCA) moves a catheter mounted balloon to specific site and inflated to displace the tissue and create a wider lumen in the blood vessel. Percutaneous coronary intervention (PCI) refers to a set of procedures like

PTCA, atherectomy, thrombolysis, intravascular radiation and correct placement of stents.

The technology of pacemakers and ICDs (cardioverter defibrillators) is evolving in terms of dual chamber activity, cost reduction, potential harmful interactions, reduction in number of leads, improved device function, advances in technology and implantation techniques. A pacemaker delivers an electrical impulse to depolarize the heart chamber in a spreading and coordinated way like a normal heartbeat. In contrast, defibrillators are used to depolarize the entire heart at once to terminate uncoordinated contractions. It is extremely useful while electric impulse conduction or initiation in the heart is blocked, slowed or triggered irregularly. The technology of artificial vascular grafts is passing through technological and clinical advancements such as endovascular therapies (angioplasty, stent), less invasive interventions for vascular repair and reconstruction, reduction in open excision and replacement, development of tissue engineered blood vessels (TEBV), performance improvement of vascular graft designs, novel coatings, improved biocompatibility and minimization of hematologic alterations. The other critical technologies are circulatory support devices for chronic congestive heart failure, artificial lungs, intra-aortic balloon pump (IABP), ventricular assist devices (VADs) and total artificial hearts (TAH). The technology is evolving with the advancement of electronics and software engineering. IABP requires that a patient maintains some native pumping capacity. A cardiac transplant is the last resort for critical patient care which fails conventional medical and surgical treatment. But, the supply of donor organs is limited today.

Artificial limbs **: Is it possible to design artificial limbs from the concept of robotic arms? what are the similarities and differences? What are the mechanical constraints: size, weight and power? What are the other design constraints: interface between artificial limbs and human body, sensors, strong light weight materials for prosthetic socket and interfaces; how to mimic the functions of biological limbs of human beings from the perspectives of ease of use, comfort and flexibility? what should be the system control mechanisms? Is it possible to design artificial limbs through CAD / CAM software? An intelligent system analytics is expected to resolve these issues accurately.**

Case analysis for biomedical technology innovation : **Let us consider three emerging technologies based on biomedical instrumentation, computer science and AI : (a) Laser therapy, (b) Wearable & Pervasive computing and (c) Surgical robots. These technologies may be interesting and good solutions for cancer care in future.**

Laser therapy for cancer care **: This section analyzes the emerging trend of laser technology for various biomedical applications such as dental problems, piles, fissures and fistula [63]. In previous session, we have already shown the application of laser for cancer care alongwith details of various advantages. In case of dental problems, smart diode laser is effectively used for the treatment of both hard and soft tissues with utmost care, precision, consistency, speed and control. The diode laser is a solid state semiconductor which produces laser wavelength (e.g. 980 nm). Laser therapy is minimally invasive, less painful, takes shorter time, reduces**

number of seating and ensures better healing and changes the experiences of the dental patients positively.

This laser system uses two wavelengths of 635 nm and 980 nm through transmission or absorption effects. 635 nm shows excellent photo biological effects due to high transmission in water. It is also optimally selected for photochemical effects and local ozone therapy activated by tolonium chloride. 980nm wavelength shows high soft tissue absorption efficiency and excellent safe surgical results for soft tissue cutting at low power radiation. Smart diode laser is expected to be cost effective (e.g. low operating cost), light weight, easy to handle, supporting preset procedures and customized programmes; equipped with large touch screen and LCD display, high storage space and advanced security features. 980 nm 10W is used for *soft tissue cutting* (e.g. coagulation, gum contouring and reshaping, gingive retraction, Haemostasis in gingival sulcus for prosthodontics impression, exposure of implants, lingual and fabial frenotoma and frenectomy, abscess opening, Epulis papiloma and fibroma removal periodontology, elimination of bacteria in periodontal pockets endodontic, sterilization of root canal and closure of microhannels); *aesthetic dentistry* (e.g. power bleaching of viral and non viral teeth) and *biostimulation* (e.g. wound healing, root canals, support in treatment of periapical lesions, periodontitis and periimplantitis, decontamination of cavities before filing treatment of chronic and recurrent aphthae, hygienisation of cervical area after scaling) and photoactivated disinfection (e.g. : root canals, periodontal pockets, support in the treatment of periapical lesions, periodontitis and periimplantitis, decontamination of cavities before filing treatment of chronic and recurrent aphithae, widespread and local inflammation of the mouth caused by herpes virus).

Diode laser therapy offers various types of benefits such as less invasive, less painful, less bleeding, less trauma, faster healing, no scars , less time (e.g. not more than an hour) and can be treated in an ambulatory condition with local anesthesia. It provides the choice of two specific wavelengths: 980nm, 10/15 W for haemorroids and fistula as safe and efficient absorption coefficient and 1470nm, 15W for varicose vein and 2 types of fibres with open end or radial. It is a cutting edge technology; has low operating cost, very compact and small sized device and may have extendable database of predefined therapy protocols and flexible customized parameters. In case of fistula, laser energy is delivered via radial fibre into the anal fistula tract and is used to thermally ablate and close off the abnormal pathway. It gives good control to the operator in surgical operation and ensures fast healing process. The tissue is destroyed and the fistula tract collapses to a very high degree. So, laser therapy can be effectively used for colone cancer care.

***Pervasive and wearable computing for cancer care* : One of the most promising emerging digital technology is health monitoring smart wearable systems (SWS) through advances of microelectromechanical systems, electrical simulation, mechatronics, sensors, actuators, biomedical instrumentation and nanotechnology. SWS is an interesting cost-effective solution which can monitor a patient's health status in real-time and support complex healthcare applications for disease prevention, symptom detection and medical diagnosis. Let us consider the structure of smart wearable system (SWS). The system may have various types of digital and mechatronics components such as sensors, actuators, power supplies, wireless**

communication and processing units, algorithms, software, UI and smart fabrics to capture and process data and make intelligent decisions based on the measurement of various parameters of human body such as temperature, blood pressure, heart rate, respiration rate, blood oxygen saturation, EEG and ECG. The measured data are sent to a central node (e.g. PDA, medical centre) through wireless communication system. SWS is expected to monitor the state of the health of human agents (e.g. patients, athletes), issue alerts and send feedback to the medical staff in real-time. The healthcare experts and consultants can take rational decisions on patient care accordingly. There are various issues and challenges in wearable and pervasive computing, telecare, tele-health and telemedicine through new models, prototypes, test beds and industrial products to enhance the performance of healthcare system and minimize the risk of illness, injury, inconvenience and rehabilitation. There are some constraints in terms of high cost, size, weight, energy consumption, complexity of sensor implementation and connectivity, ethics, laws, information security and privacy, freedom, autonomy, reliability, consistency, safety and service issues.

***Surgical robotics for cancer care*: Artificial intelligence simulates human intelligence and develops algorithms that can learn and perform intelligent behavior with minimal human intervention, high precision, accuracy and speed. Robotics is an interdisciplinary branch of mechanical, electrical and electronics engineering and computer science. Various domains of AI are used in medical robotics such as computer vision, edge computing, deep, transfer and reinforcement learning. A medical robot is a programmed machine designed to execute one or more tasks automatically and repeatedly with speed and precision for delicate and complicated surgical operations where human skills may not be applicable appropriately. The basic objectives of medical robotics are design, construction, operation and use of robots and related information system for control, feedback and information processing and development of sensors and human robot interface. The critical components of a robot are controller or brain run by a computer program; robotic operating system; electrical parts such as motors, sensors for sensing and touch, power sources: batteries, solar power; mechanical parts such as actuators, effectors, grippers, manipulators, locomotion devices, air muscles, muscle wire, pistons, grippers, wheels, and gears that make the robot move, grab, turn and lift.**

SWOT analysis on various surgical methods: Robotic surgery allows surgeons to perform complex, delicate and minimally invasive surgical tasks with more precision, flexibility and control as compared to conventional methods through tiny incisions using robotic technology. Surgical robots (e.g. da Vinci Surgical System) are self powered, computer controlled devices that can be programmed to aid in the positioning and manipulation of surgical instruments. The system includes a camera arm and mechanical arms with surgical instruments. The surgeon controls the arms while seated at a computer console near the operating table. The console gives the surgeon a high definition and magnified 3-D view of the surgical site. The surgeon leads other assisting team members. There are various types of benefits as compared to conventional open surgery such as enhanced precision, flexibility and control, transparency in view, minimally invasive prostate and heart surgery, safe, fewer complications (e.g. surgical site infection, less pain and blood loss, quicker

recovery, smaller, less noticeable scars). Medical robotics is being widely used in USA and Europe. But, there are several constraints such as skill, knowledge and cost. A single robot may cost $2'. There may be risk of death in critical cases. Robotic surgery may cost $3,000 - $6,000 more than traditional laparoscopic surgery. Robotic surgery offers a greater range of motion and precision, less bleeding and post operative pain as compared to laparoscopic surgery. Is it really possible to replace surgeons by robots in future?

Dr. Nissim and Dr. Harvey are trying to solve a puzzle. The Global Health Forum Organization is expected to redefine and implement global healthcare policy for improved immunity : "Healthcare for all at reasonable cost and optimal quality of service maintaining rationality, fairness, correctness, transparency, accountability, trust, reliability, consistency, commitment and safety through collaborative and collective intelligence". How to code the program for sustainable physical, mental and social health globally? It is rational to adopt a set of intelligent information and communication technologies for epidemic and pandemic outbreak control:

- ***Artificial immune mechanism***
- ***Intelligent broadcast communication protocol***
- ***Intelligent analytics : Real-time online data tracking system, Data mining system (e.g. Bio-informatics)***
- ***E-governance system* : Online grievance or complaint registration and tracking system for municipal corporation and gram panchayet**

Artificial Immune System : Human immune system is an adaptive, robust, complex and distributed information processing system which protects the health of the biological system from the attacks of malicious foreign pathogens (e.g. virus, bacteria, fungi, protozoa, parasitic worms). It discriminates self from non-self elements. The immunity is either innate or adaptive; innate immunity detects and kills specific known invading organisms; adaptive immunity, responds to previously unknown foreign organisms. The challenge is how to balance innate and adaptive immunity effectively. Let us try to develop Artificial Immune System.

Artificial Immune Mechanism

***System* : Biological system of human agents; life-science supply chain, healthcare service chain;**
***Input* : A self-set $S \subseteq U$, a monitoring set $M \subseteq U$ for a given system parameters;**
***Output*: for each element $m \in M$, either self or non-self / danger or normal;**

```
D ← set of detectors that do not match any $s \in S$.
for each $m \in M$ do
        {
           call threat analytics ($A_h$) → sense danger signal;
           secure function evaluation → verify innate and adaptive system immunity
        $i = f(a_h, b_h, c_h, d_h, e_h)$;
        }
sense-challenge-respond to system immunity resiliently;
```

if m matches any detector d∈D then identify m as non-self;
else identify m as self;
check if non-self or suspicious element is benign or malign danger;
if it is malign then quarantine and suppress it else give alert for social distancing;.

***Moves* :**

- ⊕ **Define *system immunity* (S_i) in terms of innate or natural immunity and adaptive immunity (humoral and cell mediated)**
- ⊕ ***Sense danger signal***
- ⊕ ***Self-nonself classification***
- ⊕ ***Clonal selection***
    - ***Hotspot***
    - ***Containment area***
    - ***Cluster configuration*: red, orange and green zone**
- ⊕ **Negative selection, somatic hypermutation and suppression**
- ⊕ **Multidimensional view of *intelligent reasoning* (perception, common sense, logical, analytical, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative)**
- ⊕ ***Case based reasoning*, standardization and benchmarking of medical practice**
- ⊕ ***Testing* (PCR,PPCR,RAT)**
- ⊕ **Private search for evidence**

Complexity Analysis of AIM : Artificial intelligence (AI) is basically simulation of human intelligence. Recently, there are debates on AI. Let us consider the outlook given by Prof. Nick Bostrom in his book 'Superintelligence : Paths, Dangers, Strategies' : Today's world need to be super careful with AI because it is potentially more dangerous than nukes. Is nuclear power really safe for our society as compared with solar power? Can we forget the tragedies of Hiroshima, Nagasaki, Chernobyl and Fukushima disaster? Is it really true or an instance of rational reasoning; can we forget the contributions of artificial intelligence in engineering, medical and management science so easily? Let us look at another view of Prof. Don Perlis of University of Maryland, College Park, USA in his work 'Five dimensions of reasoning in the wild' : an intelligent reasoning system demands new data structure beyond knowledge base with envision, perception and proper assessment of a problem; reasoning is not effective when done in isolation from its significance in terms of the needs and interests of an agent with respect to the wider world. A rational reasoning system needs the support of an intelligent analytics. AI needs a balanced and holistic approach from the perspectives of collective, collaborative, machine, business and security intelligence not only in engineering technology and management science but also medical science, efficient policy formulation and iteration for global healthcare and family welfare progrmammes.

Now, let us define the problem of the present work. The basic objective is to evaluate the natural and adaptive immunity of a complex system. It is not rational to mix the concept of immunity with security. Security is an essential part of immunity; the evaluation of immunity needs the reasoning on the needs and interest of the complex system with a broader outlook. The evaluation of the immunity of a

system involves modeling, defining complete specifications and verification. First, it is essential to develop the model (m) of a system by proper representation of its various states and programs. Next, it is important to specify the properties (p) of the system through logical reasoning. Finally, it is essential to develop a verification mechanism which justifies: does the model (m) satisfies the properties (p) indicating a healthy immune system? The evaluation of immunity of a system can be done by exhaustive search of the state space (local, global, initial and goal states and state transition relations) of a system through simulation, testing, deductive reasoning, model checking and intelligent search. The procedure terminates with positive or negative answer; the positive answer indicates a healthy immune system; the negative results provide an error trace indicating incorrect modeling or specification of the system or the occurrence of malicious threats.

***Critical observation*: A biological system ensures optimal level of immunity by balancing natural and artificial intelligence based on intelligent reasoning. A human agent must have common sense healthcare knowledge base for proper biological system control through intelligent self-assessment and self-confidence i.e. how to manage self against non-self. It demands the necessity of learning the basic concept of 'immune system' through artificial intelligence. It is possible to redefine global healthcare policy based on AIM-HS mechanism. Let us analyze the AI moves for this mechanism through a set of puzzles.**

***Move 1* : Multidimensional view of intelligent reasoning should be based on rational selection of single or multiple techniques from the list of logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative and perception based reasoning. AI reasoning is a consortium of methodologies that works synergistically and provides flexible information processing capability for handling ambiguous situations in healthcare domain. The basic objective is to exploit the tolerance for imprecision, uncertainty, approximate reasoning, and partial truth in tractable, robust and low cost solutions. Let us review the scope of these reasoning techniques to ensure health security.**

Puzzle : Can perception be an effective reasoning technique for improved immunity?
A doctor can use both complex perception based fuzzy information and simple measurement based crisp information for intelligent decision making in patient care. Even, a patient can take critical healthcare decisions in time based on perception. But the hard question is how to evaluate the positive or negative impact perception on the immunity of a biological system? Human agents can perform different types of physical and mental tasks without any measurements and any computations based on common sense reasoning or heuristics. Heuristics are intuitive knowledge or thumb rules learned from experience. In healthcare domain, a doctor can understand the medical problems of the patients and recognize symptoms, similarities and dissimilarities through the perception of time, distance, force, direction, shape, color, odor, taste, number, possibilities, likelihood, truth and other different types of attributes of physical and mental objects. Perception is the

basic building block of approximate reasoning. Recognition and perception are closely associated. Recognition is a sequence of decisions, decision are made based on information and the information is a mix of measurements and perceptions. Measurements are crisp (e.g. Body weight is 60 kg.) while perceptions are fuzzy (e.g. body weight is normal). Perception may be converted into measurements but such conversions may be counterproductive, unrealistic and infeasible. Alternatively, perceptions are converted into propositions expressed in natural languages such as a patient is very weak. Can relaxation music, yoga and meditation be a good solution for the treatment of mental health though the entertainment world is getting flooded with boom boom digital dhamaka!

Robots are increasingly used for complex surgical operations such as brains, eyes, hearts and hip replacements. Intelligent robotic walkers and toys are used for elderly and handicapped people. Robots are equipped with sensors for perceiving their environment and effectors with which they can assert physical forces on their environment. Perception is the process by which robots map sensor measurements into internal representations of the environment. Perception is a complex process as the sensors are noisy and the environment is partially observable, unpredictable and dynamic. Robots have e problems of state estimation or filtering. Good internal representations imply that robots have sufficient information to make good decisions, they are structured and updated efficiently and they are natural. Machine learning plays an important role in robot perception.

Puzzle : Can you explore the impact of forward chaining, backward chaining, uncertainty, probabilistic and imaginative reasoning on the immunity of a biological system?

The effectiveness of reasoning depends on various factors : knowledge base, sound and complete logic, inference rules, intelligence and decision making capability of agents and knowledge representation technique. In complex decisions, the expert knowledge may not be expressed in terms of single rules but in the form of chaining multiple rules together based on available data. There are two approaches of inferencing such as forward and backward chaining. Forward chaining views IF part of a rule first and the rule makes conclusion when all IF conditions are met. Backward chaining is the reverse of forward chaining. It starts from the conclusion and then identifies the IF conditions. A human agent can assess the risks on the immunity of the biological system through learning from examples i.e. supervised learning, unsupervised learning, forward chaining, backward chaining, uncertainty, probabilistic and approximate reasoning. Probabilistic reasoning evaluates uncertainty which may be inescapable in complex, nondeterministic or partially observable environments. Probabilities indicate inability of an agent to reach a definite decision; summarize the agent's beliefs with respect to the evidence. It is important to combine the agent's beliefs and desires and fix the best action plan that can improve expected utility. Let us consider a hypothetical case on envisioning i.e. imagination or anticipation of alternatives. A kid was treated with antibiotics as per treatment plan A (say allopathic). The kid was affected with chronic skin allergic disorder due to the side effects of antibiotics. His parents took the decision to shift

from treatment plan A to plan B (say homeopathic). The kid recovered from the allergic disorder. After one year, the kid was affected with diphtheria, pneumonia and chicken pox sequentially. He was shifted to treatment plan C (allopath). He was injected with a serum of bactriofuz virus which was used to kill bacillus diphtheri bacteria. Later, he had taken injections for three consecutive years to resist the effect of bactriofuz virus. The kid was recovered from all these diseases successfully. This case shows clearly how intelligent reasoning is important for correct decision making against immunological problems.

Puzzle : Can case based reasoning be an efficient technique for improved immunity?

Case based reasoning (CBR) **is a methodology for solving problems by utilizing previous experience. It involves retaining a memory of previous healthcare problems and their solutions and solving new problems by referencing the past cases. A healthcare expert presents a new query case to CBR system. The system searches its memory of past cases stored in case base and attempts to find a case that has the same problem specification of the current case. If the system does not find an identical case in its case base, it will attempt to find the case or cases that match most closely to the current query case. There are two different types of search such as similarity search and neighborhood search. In case of similarity search, the solution of the retrieved case is directly used for the current problem. The system adapts the retrieved cases if the retrieved case is not identical to the current case. In a complex search, the system requires the access of multiple case bases which are located at various locations. Let us consider a simple CBR protocol.**

CBR is selected for healthcare information system due to various reasons. The healthcare domain has an underlying model, the process is not random and the factors leading to the success or failure of a solution can be captured in a structured way. Cases recur in healthcare domain though there may be exceptions and novel cases. Healthcare solutions can be improved through case retrieval and case adaptation. Relevant healthcare cases are available at different healthcare institutes; it is possible to obtain right data. Case retrieval is the process of finding within the case base those cases that are the closest to the current case. There must be criteria that determine how a case is evaluated to be appropriate for retrieval and a mechanism to control how the case base is searched. Most often, an entire case is searched. But, partial search is also possible if no full case exists.

A *case* is a record of a previous experience or problem in terms of problem definition, patient's symptoms, drugs, solution methodology, test results and recommendations. A case base also stores global best practices, standards, valid drugs, price and contacts of specialists. Data is stored based on domain knowledge and objectives of the reasoning system. The cases should be stored in a structured way to facilitate the retrieval of appropriate case when queried. It can be a flat or hierarchical structure. Case indexing assign indices to the cases for retrieval and comparisons. There are different approaches of case retrieval. In case of nearest neighbor search, the case retrieved is chosen when the weighted sum of the features that match the query case is greater than the other cases in the case base. A case that matches the query case on n number of features is retrieved rather than a case

which matches on k number of features where k < n; different features may be assigned with different weights. Inductive approach is driven by a reduced search space and requires reduced search time. This results reduced search time for the queries. Knowledge based approaches select an optimal set of features of case by using domain knowledge. The complexity of case retrieval depends on multiple factors: (a) number of cases to be searched, (b) domain knowledge, (c) estimation of the weights for different features and (d) case indexing strategy.

Case adaptation **is the process of translating the retrieved solution appropriate for the current problem; it adds intelligence to the recommendation process. There are various approaches of case adaptation. The retrieved case can be directly used as a solution to the current problem without any modification. Otherwise, the retrieved solution should be modified according to the current problem. The steps or processes of the previous solution can be reused or modified. The solution of the current case can be derived by combining knowledge of multiple retrieved cases. Case adaptation is a complex decision making task, it considers multiple factors: how close is the retrieved case to the query case? How many parameters are different between the retrieved and the query case? DMAs can apply common sense or a set of rules or heuristics for case adaptation.**

Making sense of the information found during an investigational web search is a complex task of case based reasoning. ***Sense making*** **is to find meaning in a situation; it is the cognitive act of understanding information. The system should support collaborative information search by providing several rich and interactive views of the search activities of a group. One of the problems facing HCI research today is the design of computer interfaces to enable sense making of the processed information. Sense making is not only important for individuals, but also for groups to achieve shared goals. Traditional sense making tools focus on data mining, provide better information representation, visualization and organization of search results. But, it is also required to support the collaboration and communication that occurs among the investigators when they make sense of information together.**

Move 2 **: Define system immunity (S_i) in terms of innate or natural immunity and adaptive immunity (humoral and cell mediated); sense negative selection, danger signal detection, clonal selection, somatic hypermutation and suppression;**

Move 3 **: Define collective intelligence in terms of system dynamics (scope, input, output, feedback, process, agents), local and global healthcare policy, immunization programmes, benchmarked and standardized medical practice and education, common sense healthcare and hygiene (system control, self confidence: how to manage self? self assessment and monitoring, family planning), resource planning, efficiency of life-science supply chain and healthcare service chain;**

AIM-HS can explore collective intelligence in terms of proper coordination and integration among system, security, strategy, structure, staff, skill, style, shared vision, service and social networking. It is a hard problem. It requires proper surveillance of life-science supply chain and healthcare service chain. The basic objective is to ensure that different organizational elements of the healthcare service provider are appropriately synchronized and work in harmony to improve the

quality of service. The hard elements are strategy, organizational structure and system. The soft elements are leadership style, resources, skill, security and shared values. The hard elements can be identified and defined in a relative simple way and directly controlled by corporate management. The soft elements are difficult to define, less tangible and influenced by corporate culture. The strategic fit among these factors is the basic building block of the effectiveness of a complete and sound global healthcare policy. A system acts rationally against bio-terrorism when these ten elements are aligned correctly and mutually reinforcing.

Move 4 **: Define machine intelligence in terms of (preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, accuracy, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states) for bio-medical instrumentation and digital transformation, artificial organ transplantation (brain, heart, blood, neural system, stomach, liver, kidney, pancreas, limbs, bone marrows), wearable computing, pervasive computing and biosensors, nano-medicine and surgical robotics;**

Puzzle **: Can you assess and mitigate the risks of artificial organ transplantation on the immunity of a biological system ?**

Let us first imagine of artificial blood or blood surrogate or blood extender which can mimic and fulfill the function of natural blood. Still today, it is hard to synthesize natural blood with its oxygen carrying capability due to its complex composition. Imaginative AI reasoning envisions perflorocarbons (e.g. perfluorodecalin) as blood substitutes. But, is it possible to assess the threats of blood substitutes on the immunity of the biological system in terms of toxicity, blood group matching, malicious biological activities, retention time in the body and dissolving capability of gases like oxygen and carbon dioxide?

Next, let us consider the risks of transplantation of natural organs on the immunity of the biological system. Organ donation scheme saves life by replacing diseased organs with the healthy ones. At least seven live may be saved if a person is able to donate organ. Some organs may not be suitable for transplant such as heart, kidneys, liver, lungs, pancreas and small intestine. Such life saving organs can be only donated in case of brain death whereas tissues can be donated after cardiac death. But, can you imagine the risk of organ donation scheme from the angle of immunity? Organs can be transplanted from one person or an animal (e.g. dog, monkey, donkey, pig, goat, cow, horse and buffalo) to the sick patient. But, there is high risk of immunity problems due to transmission of deadly diseases (e.g. HIV, blood cancer). But, the problem of blindness can be resolved through transplantation of eyes; the same may be a good solution for the disorder of kidney. The society needs advanced and cost effective eye bank, blood bank and public awareness programmes of organ donation to solve critical illness.

AI has imagined the product concepts of highly complicated and costly artificial human organs such as artificial brain, heart, lungs, stomach, kidney, liver, pancreas, intestine, limbs, neural system, blood and cells though there are

technological limitations and financial constraints of biomedical electronics, instrumentation, mechatronics, robotics, computational intelligence and materials science and also critical immunity issues. It is hard to develop and simulate artificial organs due to the inherent complexities of structure, material and mechanisms of human organs. There are various risks of adaptive immunity and transmission of deadly diseases in artificial organ transplantation, artificial reproduction, common immunization programmes and breast milk feeding to the infants. AIM may be able to overcome some of those practically feasible constraints of the aforesaid imaginative reasoning through intelligent analytics and reasoning. AI community needs a new broad outlook, imagination and dreams to solve a complex problem through a set of simple mechanisms. Is it possible to evaluate the impact of artificial organ transplantation on the immunity of biological system correctly? Is it possible to synthesize artificial enzyme and hormones for the treatment of pancreatic or diabetic disorder?

Move 5 **: Define collaborative intelligence and assess its impact on the immunity of biological system in terms of information sharing principle, negotiation protocol and planning, intelligent broadcast protocol, organ donation and breast-milk feeding for childcare;**

Puzzle **: Can you assess and mitigate the risks in breast milk feeding by the mothers on the immunity of their children?**
The simple act of breast feeding a new born is the first step towards a healthy human being and has a huge impact on the health of an individual throughout his or her life-time. As per UNICEF, it provides them with essential nutrients, antibodies and protection from diseases. An intelligent imaginative reasoning can explore the risk of breastfeeding for IVF mothers, HIV affected mothers, working women and special cases due to the hormonal deficiency and problem in growth and development of breast organs due to life-style, physical and mental stress, mal-nutrition, drug addiction, alcoholism and other various factors. Some weak babies can not suck breast milk due to disorder of tongue. Can you imagine any alternative solution or product concept mapping of breast milk feeding to the infant? Privacy and trust management is a critical issue for artificial reproduction: how to store sperm and ovum correctly and fairly for test tube baby! There may be risk of incorrect swap. The worst case may be resolved through adoption of kids. Life is full of problems; but one can explore alternative solutions through intelligent reasoning.

4. STRUCTURE

Structure analytics
Agents : System analysts, scientists, engineers;
Moves**: Design and configure**

- **Organization structure**
    - **Technology and medical science forums**
    - **National level : Government, NGOs, research organizations, ;**

    - **International level : strategic alliance among global organizations (nations, health, child);**
- **System architecture ; Innovate a set of emerging technologies as per the goals of healthcare security;**
    - ***Level 1*: Biomedical, biotechnology, pharmacy, pharmaceuticals, information technology, electrical, electronics, chemical, mechanical and civil engineering;**
    - ***Level 2*: Identify fundamental building blocks of information technology - Computing schema, Data schema : database, big data analytics; Networking schema : web connectivity; security schema, application schema.**

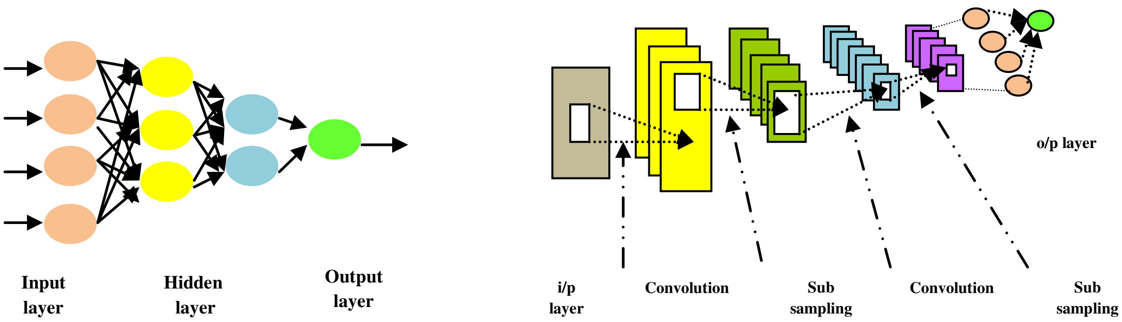


Figure 5.2: Deep learning architecture

Dr, Jim Morrison, Prof. Michel Bolton and Prof. David Nissim are analyzing the structure of the systems for health security. The first issue is *DNN System Architecture*: There are several classes of deep learning architectures used for biological data analysis. A convolution neural network (CNN) has a deep architecture with several convolutional and sub-sampling layers. Stacked auto-encoder consists of multiple sparse autoencoders. A deep belief network (DBN) freezes the weights of previous layers and feed the output to the next layer. Restricted Boltzmann machine includes a visible layer and a layer of hidden units. Mammography is a method to screen breast cancer. Breast masses are often misdiagnosed due to variability in mass appearance and low signal-to-noise ratio. Convolutional Neural Networks can be an interesting option to classify breast masses in mammograms as benign or malignant using transfer learning, and efficient data processing strategies.

Deep learning represents a class of machine learning techniques that exploit many layers of non-linear information processing for supervised or unsupervised feature extraction and transformation, pattern recognition (e.g. classification). It is used for learning multiple levels of representation to model complex relationships among data. Higher level features and concepts are defined in terms of lower level ones and such a hierarchy of features is known as deep architecture. Deep learning is based on learning representations. An observation such as an image can be represented in many ways like a vector of pixels, but some representations make it easier to learn

from examples. Deep learning is a set of algorithms in machine learning to learn in multiple levels and at different levels of abstraction. It typically uses artificial neural networks such as multi-layer feedforward neural network and convolutional neural network.

There are three classes of deep learning architectures and techniques: (a) Deep networks for unsupervised or generative learning, (b) Deep networks for supervised learning and (c) hybrid deep networks. Unsupervised learning is used to capture high order correlation of the visible data when no information about target class labels is available. In case of supervised learning, target label data are always available in direct or indirect forms. Hybrid deep networks use both unsupervised and supervised learning techniques. Many machine learning techniques use shallow structured architectures consisting of at most one or two layers. Shallow architectures are effective in solving simple problems are not effective for complicated applications due to limited modeling and representational power. Human information processing mechanisms needs deep architectures for extracting complex structure and building internal representation from rich sensory inputs. The basic concept of deep learning comes from the domains of ANN, AI, graphical modeling, optimization, pattern recognition and signal processing. Deep learning has several advantages as compared to shallow architecture: increased chip processing abilities, significantly increased size of training data and recent advances in machine learning research have enabled the deep learning methods to exploit complex and nonlinear functions, to learn distributed and hierarchical feature representations and effective use of both labeled and unlabeled data.

Deep Learning is basically credit assignment in adaptive systems with long chains of causal links between actions and consequences. It is accurately assigning credit across many stages. A standard neural network consists of many simple connected processors or units each producing a sequence of real valued activations. Input units get activated through sensors perceiving the environment, other units through connections with weights from previously active units. Learning or credit assignment is to find weights that make the neural network exhibit desired behavior. A complex problem may require long causal chains of computational stages. Convolution Neural Networks (CNN) architecture are widely used for computer vision. The receptive field of a unit with given weight vector is shifted step by step across input values. The resulting array of subsequent activation events of a unit can provide inputs to higher level units.

The next critical issue is the structure of biomedical devices. The topology of technology should be analyzed in terms of circuit intelligence: nodes, connectivity, type of connections; layers, interfaces between layers and organization of layers. Today, it is hard to perceive a concrete picture of the aforesaid artificial biomedical devices from conceptual stage. The system architecture of the aforesaid biomedical devices is not yet transparent; it is not a simple design. The architecture depends on the mechanism of the biomedical device; and also computing, data, networking, application and security schema.

***Tissue engineering* is expected to be a good solution to the innovation of aforesaid artificial organs (e.g. artificial kidney, liver and pancreas) through cell and gene**

therapies. It is an emerging trend of biomedical engineering; the basic building blocks are cellular, organ and molecular biology, biotechnology, chemical and mechanical engineering and material science. It may be possible to reconstitute, maintain, simulate and improve tissue or organ functions in building artificial organs. It is an interesting research agenda whether it will be possible to replace physiological functions of diseased tissues and living organs with synthetic materials, biological compounds and cells. Finally, the expert panel are focusing on the structure of artificial immune system.

- ***Artificial immune system***
- ***Intelligent broadcast communication system***
    - ***System*** **: Radio, TV, Mobile phones, Social networking system, Knowledge management system;**
    - **The sending agents broadcast data on epidemic assessment and mitigation plan, symptoms and causes of diseases.**
    - **The receiving agents verify the security intelligence of broadcasted data such as false data injection, shilling and Sybil attacks.**
- ***Intelligent analytics***
    - ***Real-time online data tracking system***
        - ***Real-time data tracking system of available healthcare services*** **(e.g. free beds, paid beds) in hospitals and clinics at a particular zone (e.g. city, rural area, district);**
        - ***Real-time data tracking system*** **of stock (or inventory) of medicines in retail outlets of drugs and medicines;**
        - ***Real-time data tracking system on epidemic and pandemic outbreak*** **(e.g. [zone, country, state, district], infection, testing, recovery, death, suspected agents, prediction);**
- ***E-governance system*** **: Online grievance or complaint registration and tracking system for municipal corporation and gram panchayet**
    - ***Access online portal.***
    - ***Input :*** **Enter personal data (name, address, phone number, email address, ward no.), complaint details (infection, death, gaps in municipal functions e.g. cleaning of drains, removal of garbage).**
    - ***Output*** **: Get complaint registration number.**
    - ***Test, trace and track*** **the status of action by municipal corporation / pnnchayet against complaint number.**
- ***Telemedicine*** **for treatment of epidemic and pandemic outbreak**

Theorem **: AIM verifies innate and adaptive system immunity in terms of collective, machine, security, collaborative and business intelligence through multi-dimensional view on intelligent reasoning.**

The proposed mechanism (AIM) is defined by a set of elements : system, a group of agents, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payment function, an optimal set of moves, revelation principle and model checking or system verification

protocol. The proposed mechanism evaluates the innate and adaptive immunity of a system which is defined by a set of states (e.g. initial, goal, local and global) and state transition relations.

The mechanism follows a set of AI moves. The basic building block of the mechanism is an analytics having multidimensional view of intelligent reasoning. Reasoning has multiple dimensions like common sense, automated theorem proving, planning, understanding, hypothetical, simulation dynamics and envisioning i.e. imagination or anticipation of alternatives. The inference engine selects appropriate reasoning techniques from a list of options such as logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative and perception based reasoning depending on the demand of an application. Another important move is the collection of evidence through private search which may require a balance between breadth and depth optimally. It is computationally hard to simulate the intelligence of a detective with high IQ in a mechanism; can you recall the reasoning style of Ace Ventura or Sharlock Homes to collect right evidence for solving critical cases!

The critical challenge is how to detect the danger signal from a system? The mechanism evaluates system immunity (i) combinatorially in terms of collective intelligence, machine intelligence, security intelligence, collaborative intelligence and business intelligence. The collective intelligence (a) is defined in terms of scope, input, output, process, agents and system dynamics. For a complex application, it verifies coordination and integration among system, strategy, structure, staff, style, skill and shared vision. What is being done by various components of a system? Who is doing? Why? How? Where? When? The machine intelligence (b) checks the system in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy. For example, it should check preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states and state transition plans of an information system.

The security intelligence (c) verifies the system in terms of authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy; rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, commitment, reliability and consistency. The collaborative intelligence (d) evaluates the feasibility and effectiveness of human-computer interaction to achieve single or multiple set of goals, information sharing principle and negotiation protocol. The business intelligence (e) looks after business rules such as payment function, cost sharing, bonus, contractual clauses, quality, performance, productivity, incentive policy and competitive intelligence.

The basic protocol of AIM is based on bio-inspired artificial intelligence and immunological theories such as negative selection, danger signal detection, clonal selection, suppression and hyper mutation. Negative selection is an immune inspired classification scheme. For a given set of self sensor nodes, it generates a set D of detectors that do not match with any element of S. Then, these detectors are used to partition a monitor set M into self and non-self elements. The problem faced by human immune system is similar to that of information and communication

technology schema. It is difficult to defend a system against a previously unknown danger. The only reliable knowledge is the normal behavior of the system which is equivalent to self nodes of the distributed system. Negative selection mimics the human immune system; it generates a set of detectors that do not match with self nodes, these detectors are used to monitor the abnormal behavior of the distributed system caused by the attack of non-self nodes. Danger threatens living organisms; the danger theory suggests that the human immune system detects danger to trigger appropriate immune responses. The optimal trade-off between the concentration of danger and safe signals within human tissues produce proper immune responses. Danger also threatens distributed computing systems. Danger theory can be applicable to intrusion detection. It is an interesting option to build a computational model which can define and detect danger signals. The danger signals should be detected fast and automatically to minimize the impact of malicious attacks by the intruders on a distributed system.

The mechanism verifies system immunity through a set of verification algorithms. It is possible to follow various strategies like model checking, simulation, testing and deductive reasoning for automated verification. Simulation is done on the model while testing is performed on the actual product. It checks the correctness of output for a given input. Deductive reasoning tries to check the correctness of a system using axioms and proof rules. There is risk of state space explosion problem in case of a complex system with many components interacting with one another; it may be hard to evaluate the efficiency of coordination and integration appropriately. Some applications also demand semi-automated and natural verification protocol. The mechanism calls threat analytics and assesses risks of single or multiple attacks on the system under consideration: analyze performance, sensitivity, trends, exception and alerts; checks what is corrupted or compromised: agents, protocol, communication, data, application and computing schema? Performs time series analysis: what occurred? what is occuring? what will occur? assess probability of occurrence and impact; explores insights : how and why did it occur? do cause-effect analysis; recommends : what is the next best action? predicts: what is the best or worst that can happen?

***Theorem*: The computational intelligence is associated with the cost of verification algorithms of system immunity and the complexity of threat analytics.**

The verification system requires both automated and semi-automated verification options. The verification system calls threat analytics and a set of model checking algorithms for various phases : exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of the system under consideration. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

There are two different phases : explanatory phase to locate errors and fault finding phase to look for short error trails. Model checking is an efficient verification technique for communication protocol validation, embedded system, software programmers', workflow analysis and schedule check. The basic objective of the model checking algorithm is to locate errors in a system efficiently. If an error is found, the model checker produces a counter example how the errors occur for debugging of the system. A counter example may be the execution of the system i.e. a path or tree. A model checker is expected to find out error states efficiently and produce a simple counterexample. There are two primary approaches of model checking: symbolic and explicit state. Symbolic model checking applies to a symbolic representation of the state set for property validation. Explicit state approach searches the global state of a system by a transition function. The efficiency of model checking algorithms is measured in terms of automation and error reporting capabilities. The computational intelligence is also associated with the complexity of threat analytics equipped with the features of data visualization and performance measurement.

The computational intelligence may be associated with four decisions depending on the type of an application: encoding, similarity measure, selection and mutation. Antigens and antibodies are encoded in the same way. An antigen is the target or solution. The antibodies are the remainder of the data. After the fixing of efficient encoding and suitable similarity measure, the algorithm performs selection and mutation both based on similarity measure until stopping criteria are met.

The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the system: agents, communication schema, data schema, application schema, computing schema and protocol? what occurred? what is occuring? what will occur? Assess probability of occurrence and impact. The analysis on insights may be as follows: how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen?

4. SECURITY

Prof. Bob Taylor and Dr, Arvind Gurumurthy are analyzing the security intelligence of emerging healthcare technologies. It is essential to verify security intelligence of the technological innovation associated with cancer prevention collectively through rational threat analytics at five levels : L1, L2, L3, L4 and L5. At level L1, it is important to audit the access control mechanism for the biological system of cancer patients in terms of authentication, authorization, correct identification, confidentiality and data integrity. At level L2, it is required to verify fairness, robustness, correctness, transparency, accountability, trust and commitment. Next, it is required to verify the system performance at level L3 in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety. At level L4, it is required to assess

the risks of various types of malicious attacks by adversaries on the human biological system such as Denial of Service (DoS), false data injection attack and sybil attack. At level L5, it is required to assess the risks of various types of corruptions such as agents, system administration and payment function associated with cancer treatment. It is rational to adopt an optimal mix of proactive and preventive i.e. sense-and-respond approaches to fight against cancer; the following section outlines a Deep Analytics based Cancer Prevention Mechanism (DACPM).

Deep Analytics based Cancer Prevention Mechanism [DACPM]

***Agents*: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);**
***Model*: Human biological system – (a) body, (b) mind;**
***Objectives*: cancer prevention at optimal cost;**
***Constraints*: budget or financial constraint, resources, time, knowledge;**
***Input*: Perception of human agent, performance measures of biological system or test data;**
***Strategic moves*:**

- **optimal mix of proactive and reactive approaches;**
- **deep learning algorithm;**
- **intelligent reasoning : case based reasoning (CBR), perception, analytical, logical, common sense, biomedical instrumentation;**
- **rational healthcare payment function and budget plan;**
- **adaptive secure multi-party computation;**

***Revelation principle*: The agents preserve privacy of strategic data;**

- ***Defender* : The defenders share critical information collaboratively.**
- ***Attacker*: The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

***Cancer Prevention Approaches*:**

- ***Proactive approach*:**
  - **Identify targets : computing, data, networking, security and application schema;**
  - **Threat modeling**
    - **Call threat analytics function (f_a) and assess miscellaneous risk elements;**
    - **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
    - **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
    - **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**
    - **Estimate requirements of healthcare in terms of demand plan (P^p_d);**
    - **Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.**
      - **Auto-immunity and vaccination;**

- **Optimal diet intake (e.g. fruits : amla, vegetables, nutrients) to fight against malnutrition;**
- **Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities, stress control through meditation;**
- **Self-healing mechanism through wearable computing based health monitoring devices which measure several health parameters in real-time such as pulse rate, temperature, blood pressure, respiration rate, heart bit and oxygen saturation rate;**
- **Yoga for physical pain and treatment of psychological, social and spiritual trauma (as side effects of radiation and chemotherapy)**
  - **'Suryanamaskar'**
  - **'Pranayam' and deep breathing exercises for stress management**
  - **Free hand exercises for muscle relaxation**
    - **standing postures (e.g. 'chakrasan', 'pada hastasan')**
    - **sitting postures (e.g. 'ustrasan' or camel pose, 'shashangasan' or rabit pose)**

- ***Reactive approach*:**
  - **adopt sense-and-respond strategy.**
  - **assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.**
    - **what is corrupted or compromised?**
    - **time series analysis : what occurred? what is occuring? what will occur?**
    - **insights : how and why did it occur? do cause-effect analysis.**
    - **recommend : what is the next best action?**
    - **predict: what is the best or worst that can happen?**
  - **verify security intelligence of application, computing, networking, security and data schema of biological system.**
    - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**
    - **Level2: authentication, authorization, correct identification, privacy, audit;**
    - **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**
    - **Level4: stability, system dynamics, quality of application integration.**
  - **Explore risk mitigation plan (P^r_d and P^r_m).**

        - Do medical testing → Data visualization (Refer Deep Leaning Algorithm of section 2.1)
        - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
        - Integrated medicine
        - Regenerative medicine
        - Chemotherapy and radiation
        - Laser

- ***Fight against bad luck*** **: Identify critical risk elements.**
    - **Genetic disorder (sex, race, ethnicity, somatic mutation)**
    - **Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)**
    - **Injuries from accidents, sports and games, war and crime**
    - **Side effects of medical treatment (e.g. hormone therapy)**
    - **Occupational exposure (e.g. at nuclear power plant; alternative option : solar power)**
    - **Environmental pollution (e.g. nuclear and thermal power plant)**
    - **Hostile climate, weather and other locational disadvantages, exposure to sunshine**
    - **Malnutrition due to poverty**
  - **Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.**

Payment function**:**

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Cost of illness (COI) : health sector costs (direct cost) + decreased or lost productivity by the patient (indirect cost) + the cost of pain and suffering (intangible cost);**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**
- ♦ **Crowd funding campaign through social media (e.g. pediatric cancer treatment appeal at social networking site or crowd funding portal.**

Output**: Cancer prevention plan**

Deep Learning Algorithm

Objective**: Computer aided cancer detection and diagnosis with improved accuracy;**
Input **: Medical images with optimal number of correct features;**

Data preprocessing **: Filter raw data from noise and incompleteness;**
System Architecture**: Deep Convolution Neural Network (CNN);**
Training strategy **: Ensemble learning**

- **Create multiple data sets from original training data;**
- **Build multiple base classifiers (e.g. kNN, SVM, DT, RF, GBDT) for each data set;**
- **Combine classifiers;**

Algorithm **:**

```
D: Original training data , n : no. of base classifiers, $D_t$: Test data;
   for i = 1 to n do
     create training data set $D_i$ from D;
     build base classifier $C_i$ on $D_i$;
    end for
    for each test data $x \in D_t$
     $C^*(x) = C_1(x) \oplus \ldots \oplus C_n(x)$; /* $\oplus$ : combination operator */
    end for
```

Testing strategy**: Predictive accuracy analysis;**
Output**: Pattern recognition for cancer location identification, cancer tissue classification, cancer image segmentation, cancer image retrieval, big image data analysis**

DACPM is basically a security game i.e. fight against cancer. It is defined by various types of elements: a group of agents, model, actions, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payments, a strategy profile, a dominant strategy which maximizes the utility of an agent for all possible strategies of other agents involved in the mechanism, security intelligence and revelation principle. There are two agents in the security game: a defender (D) and the attacker (A). Each agent adopts and executes a or a set of strategies. A pure strategy is a deterministic policy for a single move game. For many games, an agent can do better with a mixed strategy. The best strategy may depend on the knowledge of the defender about prospective attacks and the sunk costs incurred when upgrading information security schema reactively. The payment function of the mechanism estimates an optimal investment plan for the protection of human biological system. The mechanism verifies the security intelligence of human biological system; it is a multi-dimensional parameter which is defined in terms of rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment; safety, liveness, synchronization, reachability, deadlock freeness; authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy.

The DACPM mechanism evaluates security intelligence of the human biological system based on proactive and reactive approaches. The system is expected to be a resilient system. The resiliency measures the ability to and the speed at which the information system can return to normal performance level following a disruption. Adaptability is about responding to change effectively and decisively through reactive approach: the ability to identify the change in search space for the adversaries, understanding the probable impacts of the hit by the adversaries, rapid

quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation. The vulnerability of the system to a disruptive event such as cancer should be viewed as a combination of likelihood of a disruption and its potential severity. The defender must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the defender should explore what can go wrong in the operation of the system? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences.

The defender tries to define the payment function associated with healthcare in terms of aspiration point, reservation point and adjustment of various preferential thresholds (e.g. indifference, strong preference, weak preference, veto) and preferred solutions. Cost of illness may be estimated based on direct cost (e.g. health sector costs), indirect cost (e.g. loss of productivity of the patient) and intangible cost (e.g. cost of pain and suffering). Direct costs include hospitalization, medication, emergency transport, and medical care. Decreased or lost productivity may be the result of illness, premature death, side effects of illness or treatment or time spending receiving treatment. With premature death, the indirect cost is the loss in wage and benefits.

The computational cost of deep learning mechanism depends on the complexity of threat analytics function, deep learning algorithm and payment function. The cost of computation is a function of the complexity of threat analytics. The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. Another major computational burden of the deep learning mechanism is the complexity of verification or model checking algorithms. The cost of computation also depends on the complexity of payment function. The appendix shows the application of DACPM for nine types of cancer as stated in scope (appendix).

It is essential to design biomedical devices in terms of security at various levels – L_1, L_2, L_3, L_4 and L_5. Level L_1 verifies system performance in terms of correctness of measurement of health parameters by sensors, safety, reliability, consistency, stability and robustness. The device should be safe. Safety is the most important consideration in the design of any biomedical device. Let us consider the safety aspects of artificial kidney in terms of biological, chemical, mechanical and human factors. The device should have high biocompatibility and blood compatibility; the device should not cause hemolysis i.e. destruction of red blood cells. Water quality is a major safety concern for dialysate fluid. The dialysis membrane should have high shear and ultimate strength. The device should be easy to operate and should be fool-proof. The design of artificial limbs is expected to satisfy several critical requirements such as subconscious control, user friendliness for simple learning and use, independence in multifunctional control, parallel control of multiple functions, direct access, speed of response, no sacrifice of human functional ability and natural appearance.

Security analytics for biomedical technology

- **Level 1: System performance – correctness, reliability, consistency, stability, robustness, resiliency, liveness**
- **Level 2 : Access control – authentication, authorization, correct identification, audit of quality control issues**
- **Level 3 : Design schema – safety, biological safety, mechanical safety, chemical safety, human factor safety, rationality, transparency, accountability, fairness, correctness**
- **Level 4 : Corruption – computing, data, application, networking schema**
- **Level 5 : Malicious attack - false data injection attack, data traffic congestion, denial of service**

The other critical design issues are also associated with resiliency, deadlock-freeness, synchronization and interactive intelligent communication protocol. The safety of bio-medical devices depends on access control at level L_2 in terms of authentication, authorization, correct identification of system components and audit of quality control issues. The security schema is also designed and verified at level L_3 in terms of rationality, fairness, transparency, accountability, trust and commitment.

The safety of the bio-medical devices may be threatened at level L_4 through corruption of computing, data, application and networking schema. The design of the bio-medical devices is also expected to assess and mitigate the risks of various types of attacks at level L_5 such as false data injection, shilling and data traffic congestion. A biomedical device should be safe from the perspectives of biological, chemical, mechanical, human factor safety. Safety is one of the most important design criteria. A biomedical device should have high biocompatibility and blood compatibility. For example, an artificial kidney should not result hemolysis i.e. destruction of RBC; should not adsorb or filter blood cells; should not introduce any foreign toxic materials into blood; also remove toxic material. The quality of *w*ater is a major safety concern for dialysate fluid. The dialysis membrane should have high shear and ultimate strength and dimensional stability. A biomedical device should be easy to operate and should be fool-proof. Alarms should be incorporated into a biomedical device the dialysis machine to signal any malfunctioning of the system components.

What is *bio-terrorism*? This is a question of life and death in human society globally. Traditionally, it is the intentional use of biological or chemical agents to cause disease or destroy food and water supplies or capture and kill human agents for political or economic reasons to achieve malicious business intelligence [28]. Today, it is difficult to classify the illnesses caused by biological, chemical and radiological weapons from naturally occurring ailments. Our society is going through an excellent progress of life-science supply chain management and healthcare service and medical practice. But, there is threat of bio-terrorism on the soft targets such as life-science supply chain and healthcare service chain. Bio-terrorism is basically a management game in today's business world. Bo-terrorism is generally related to the use of biological, chemical and radiological weapons in the battle fields. Most

surprisingly, the definition of bio-terrorism has been changed from the use of bullets and explosives towards slow poisoning of the innocent public through innovation of new viruses, anti-viruses, drugs and toxic tasty junk food, soft drinks and beverages, flawed digital bio-medical instrumentation and unethical medical practice. It is a silent trap of death. The conflicts between security intelligence and business intelligence are inevitable. Today's healthcare system must satisfy the basic requirements of security and safety for the benefits of the common people of the world. The analytics must explore the risk of all possible threats on the soft targets. Our society needs rational decision support system, microsoft healthcare policy and innovative medical practice to resist bio-terrorism. Is it a mission impossible? The following section outlines today's bio-terrorism mechanism transparently.

***Agents*: Service provider (P), Service consumer (C), Partners of life-science supply chain, Adversaries;**
***Input*: Data on agents, healthcare products and services;**
***Targets*: Life-science supply chain, Healthcare service chain;**

- ***Life-Science Supply Chain***
    - ***SCOR***
        - **Planning: demand, inventory, production and capacity, packaging and labeling, MRP;**
        - **Collaboration and sourcing;**
        - **Execution -sales and distribution, order management, warehouse management, transportation management, reverse logistics;**
    - ***DCOR*: innovation, product life-cycle management, pricing;**
    - ***CCOR*: customer relationship management;**
- ***Healthcare Service Chain*: registration, consulting, testing, surgical operations, billing, payment processing and follow-up;**

***Threats*: call threat analytics and assess risks;**

- **Management Information System (MIS) corruption**
    - **False data injection attack**
    - **Sybil attack**
    - **Private data leakage**
    - **Flawed web security**
    - **Flawed Knowledge Management System for creation, storage, transfer and application**
- **Broadcast corruption through shilling attack**
- **Technical snags, unreliability and inconsistency in digital bio-medical instrumentation**
- **Biotechnology based innovation of new germs, viruses and anti-viruses**
- **Life-science supply chain corruption**
    - **Good Manufacturing Practice (GMP)**
    - **Total Quality Management (TQM)**
    - **Social Choice Problems (e.g. crimes, kidnapping)**
- **Poor quality of service in healthcare service chain**

- **Transaction processing system**
- **Decision support system and GDSS**
- **Business intelligence system**
  - **Malicious data mining**
  - **Insecure data storage**
  - **False data visualization**
  - **Poor performance measurement**
- **Malicious business intelligence**
  - **Greedy heuristics in payment function for revenue and profit optimization**
  - **Economic pressure and incentive policy**
  - **Fraudulent health insurance model**
  - **Investment for technology management**
- **Irrational and dull HR policy in talent management**
- **Chaotics in formulation of public policy, mechanisms, regulatory compliance and corporate governance**

***Security intelligence verification*: call intelligent threat analytics, verify security intelligence at multiple levels.**

- ***Level 1*: audit computational intelligence in terms of correctness of computation and rationality of filter configuration,**
- ***Level 2*: verify system performance of the adaptive filter in terms of reliability, consistency, resiliency and liveness;**
- ***Level 3*: malicious attacks – verify the risks of Denial of Service (DoS), false data injection, intrusion and Sybil attack on adaptive filter;**
- ***Level 4*: multi-party corruption – assess the risks of corruption of system administrator and filtering mechanism of adaptive filter;**
- ***Level 5*: verify the efficiency of access control of adaptive filter in terms of authentication, authorization, correct identification, privacy, audit, nonrepudiation, confidentiality and data integrity;**

***Strategic moves for risk mitigation*: Scope, System, Structure, Security, Strategy, Staff-resources, Skill-Style- Support (governance and regulatory compliance, Shared vision, Service and Social networking);**
***Output*: Plan to counter bio-terrorism**

THREAT ANALYTICS

Theorem : The security intelligence is explored through threat analytics on bio-terrorism.
It is essential to verify the security intelligence of the target system (i.e. life-science supply chain and healthcare service chain) in terms of correctness, fairness, rationality, trust, transparency, accountability, reliability, consistency, confidentiality, data integrity, non-repudiation, authentication, authorization, correct identification, privacy, safety and audit. It defines the security intelligence of the system comprehensively with a novel concept of collective intelligence.

In bio-terrorism mechanism, the soft target points of adversaries may be life-science supply chain and healthcare service chain. An intelligent analytics explore miscellaneous types of threats on the targets such as information system corruption through false data injection attack, sybil attack, private data leakage and knowledge management; broadcast corruption through shilling attack; technical snags, unreliability and inconsistency in the performance of digital bio-medical instrumentation; poor quality of service in registration, consulting, testing, surgical operation, billing and payment processing of healthcare service chain; flaws of transaction processing, decision support, group decision support and business intelligence system : malicious data mining in testing, insecure data storage, data visualization techniques and performance measurement; life-science supply chain corruption in planning, collaboration, execution, sales and distribution, product life-cycle management; malicious business intelligence in the modes of greedy heuristics in payment function for revenue and profit optimization, economic pressure and irrational incentive policy, fraudulent health insurance model and financial intelligence, incorrect decision on investment for technology management; biotech innovation of new jerms or viruses and anti-viruses and finally irrational and dull human resource management policy in talent management, reward and recognition. This list is not exhaustive. There are other several critical factors such as non-cooperative corporate culture, power play and politics, ethics, strategic blunder and chaotics in formulation of public policy, mechanisms and corporate governance. It is an open research agenda.

Bioterrorism mechanism explores different scenarios of corruption in terms of service provider, consultant, service consumer, life-science supply chain partners, system administrator and adversaries. The system results correct and fair output if all the agents, communication channel and data are free of corruption. Corruption may occur in various ways. The adversary is capable of corrupting an agent, input or output data. The corruption strategy indicates when and how parties are corrupted. In case of static corruption model, the adversary is given a fixed set of parties whom it controls. Honest parties remain honest throughout and corrupted parties remain corrupted. In case of adaptive corruption model, adaptive adversaries are given the capability of corrupting parties during the computation. The choice of who to corrupt, and when, can be arbitrarily decided by the adversary and may depend on its view of the execution. The basic objective of the threat analytics is to assess risks of different types of malicious attacks and explore risk mitigation plans accordingly.

The mechanism uses 10-S model as a set of strategic moves of mitigating the risk of aforesaid threats: System, Security, Strategy, Structure, Staff, Skill, Style, Shared vision, Service and Social networking. It is a hard problem. It requires proper coordination and integration among ten elements associated with life-science supply chain and healthcare service chain. The basic objective is to ensure that different organizational elements of the healthcare service provider are appropriately synchronized and work in harmony to improve the quality of service. The hard elements are strategy, organizational structure and system. The soft elements are leadership style, resources, skill, security and shared values. The hard elements can be identified and defined in a relative simple way and directly controlled by

corporate management. The soft elements are difficult to define, less tangible and influenced by corporate culture. The strategic fit among these factors is the basic building block of organizational effectiveness. A system acts rationally against bio-terrorism when these ten elements are aligned correctly and mutually reinforcing.

Theorem : Technology management is a critical threat factor responsible for bioterrorism through corruption of management information system, corrupted communication schema, malicious bio-medical instrumentation and biotech innovation.

(*Case-1.1: Biomedical instrumentation*): This is the case of technical snags, unreliability and inconsistency in digital bio-medical instrumentation. Digital transformation requires the intelligence of biomedical engineering, bio-sensors, bio-inspired artificial intelligence and human computer interaction for improved QoS in patient care. A smart healthcare information system should be correctly integrated with bio-medical system appropriately through sensors, robotics, human computer interaction, mobile communication system and internet. An effective digital transformation enables the service provider to offer different innovative patient care services through medical imaging systems, digital radiography, computed tomography, nuclear medicine, computer-integrated interventional medicine, ultrasonic imaging, magnetic resonance imaging, diffuse optical imaging, image compression, medical image retrieval, parametric imaging, brain magnetic resonance imaging, molecular imaging, data processing and analysis by electronic medical record (EMR), image registration, biological computing, picture archiving, medical imaging informatics, digital library, integrated multimedia patient record systems, computer-aided diagnosis and clinical decision support systems. The patients or healthcare service consumers can receive innovative healthcare services through digital transformation such as mobile electrocardiogram (ECG) recording, portable defibrillators, digital X-ray, digital stethoscopes, digital pulse monitoring watches, blood pressure monitors, blood sugar monitors, pacemakers, pregnancy and urine test kits.

The most serious threat of digital biomedical instrumentation is inconsistent and unreliable malfunctioning of the devices and instruments due to intentional and planned attacks by the malicious agents. They may configure the devices incorrectly. There may be problems of regular and preventive maintenance of these devices. A maliciously configured or malfunctioning digital stethoscope or pulse watch may declare a live patient as dead. Attestation verification of biomedical devices is a critical requirement of a smart healthcare service chain as a part of regular and preventive maintenance: check if a device is tampered by an adversary; check the configuration and correct setting of each device; detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code. Each device should be attested with a valid digital test certificate. The verification algorithm must verify the identity and tampering status of each device. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of a device. A challenge response protocol should be called between a

trusted external verifier and a biomedical instrument on periodic basis to check the reliability, consistency and correctness of the system. Bio-medical instruments must use efficient pattern recognition algorithms for patter recognition such as support vector machine for pattern classification, clustering and association rule mining.

(*Case-1.2 : Biotechnology*): This is the case of biotechnology based innovation of new germs or viruses and anti-viruses. New types of jerms are explored and injected into human body through different common channels such as natural disaster (e.g. rainfall, flood), environmental pollution (e.g. air, water, soil), water supply, saline, drugs and pathological tests. It optimizes the revenue of drug companies through increased sale of anti-viruses. On the other side, it reduces the life-cycle of the patients or service consumers. It is basically a malicious management game. Cross-border medical terrorism is becoming a common occurrence in human society today; it may be across countries, inter-state, inter-district, inter-city and inter-villages. The migrants are often subjected to new drugs, medical treatment and surgical operation procedures for risky experiments in medical science. Many people are losing their life prematurely due to such terrorism. The experiment should be done on other animals through intelligent simulation game. The critical causal factor of such type of bio-terrorism is erosion of social values and quality of education at branded technical, medical and management institutes, R&D laboratories and mult-tiered life-science supply chain. The scientists innovate new medicines and biomedical instruments for the benefits of the human society; the business world often uses the innovation maliciously for greater sales, revenue and profit. It requires close watch, monitoring and audit of the activities of these institutes privately and continuously for the good of common people. Absolute autonomy in system administration and freedom of expression may result horrific disasters and chaotics in human society today.

(*Case-1.3: False data injection attack*): False data injection attack broadcasts incomplete, corrupted, noisy, got up and incorrect data through intrusion of malicious agents or corrupted sending agent and affects the reliability of corporate communication system. False data injection attack is very common through broadcast such as reproduction mechanisms, sports, body building and sex medicines, joint and knee pain killer medicines and beauty care products (e.g. skincare, hair care) without mentioning the side effects of different chemical compounds and herbal ingredients used in the medicines on human health and mind. A patient can be easily confused and cheated through popular broadcast and digital advertising. For example, detailed ingredients and chemical compositions are not mentioned clearly on the packet of drug Z for hair care though it is very costly product. The public are consuming energy capsules unknowingly and getting attacked with ailments of digestion system, liver and kidney.

The service consumers must verify the fairness, trust and correctness of data communicated by the service provider to detect false data injection attack and mitigate the risk through social choice. The verification mechanisms require the intervention of trusted third parties or detectives who should arrest the malicious agents. The recipients must adopt tit-for-tat strategy: honest public campaign

against fake broadcast, threats and punishments of the adversaries. The service consumers must verify the quality of broadcast and provide true, honest and intelligent feedback to the broadcasting forum. If the forum is inactive, toothless, clawless and casual, the deceived agents should report to the highest authorities and seek for legal help to corporate governance. The recipients may adopt retaliative moves such as rejection of fraud channels or switching from one service provider to the other for better quality of service.

(*Case-1.4: Shilling attack*): This is the case of broadcast corruption through shilling attack. Adaptively secure broadcast is essential to resist shilling attack. Malicious broadcast is a real threat to the digital advertising world. If the recipients sense flaws in digital advertising, the system administrator must verify the correctness, fairness and transparency of the system through analytics on ad slot allocation, content of adwords, exposure time and frequency, customization, delivery, click rate, and impression. Today's broadcast is closely associated with advertising as a recommender system. But, there is risk of *shilling attack* in the form of *push* and *nuke* attacks where the rating of target items (e.g. drugs, medicines and cosmetics) are increased and lowered successively. The advertising world may be digitally divided with a flavor of revenge and retaliation due to zero or low investment on advertising by the corporate world. A corrupted broadcasting system may be involved in brand dilution of a good company through baseless, mischievous and false propaganda. Alternatively, the broadcasting system can push a set of targeted items of poor quality and brand to the public through fraudulent adwords, euphemism and attractive presentation of the popular brand ambassadors. But after the disclosure of the information on such types of malicious attacks, the recipients may lose their trust in the adwords of the digital world in future.

This is the most dangerous threat on a broadcasting system where the sender and the recipients may be honest but the sources of broadcasted data are corrupted. The recipients must threaten and refuse false adwords and complain to the broadcasting forum, quality control and detective agencies and government authorities in time against fraudulent business intelligence. The profiles of shilling attackers must be deleted with the help of collaborative filtering and efficient ranking system. The problem should be solved through regulatory compliance (e.g. RTI, consumer protection acts), cryptology and network security jointly.

(*Case-1.5.1 : Sybil attack on cancer treatment*): This is the case of cancer treatment today. The patients are treated incorrectly and diagnosed as cancer casually though there is another simple medical problem. Natural intuition and perception are not applied for simple medical problems. The patients are incorrectly recommended for costly treatment. They are often recommended for costly treatment procedure repeatedly (e.g. CT scan, X-ray), drugs and surgical operations. The poor and helpless patients are forced to validate and verify the test reports and medical diagnosis at various healthcare institutes. This is an instance of modern biological, chemical and radiological terrorism. Fairness and correctness of computation and testing is a critical concern in healthcare practice. Knowledge management is

another critical success factor; case based reasoning may be a good solution for correct clinical decision making.

(*Case-1.5.2 : Sybil attack on herbal and unani drugs*): Herbal and Unani drugs are often sold at very high price in the market in the form of sophisticated labels and packaging of scientific drugs. The poor patients are forced to spend high amount of money on account of fake drugs. The consumer protection ministry should detect this fake drug racket to save the people. If a herbal or ayurvedic or unani drug is really effective for a healthcare problem; it should be recognized through proper channel, marketing, branding, pricing, promotional and distribution strategy.

It is really complex to trace the corrupted players in the broadcast. A broadcasting communication network is defined by a set of entities, a broadcast communication cloud and a set of pipes connecting the entities to the communication cloud. The entities can be partitioned into two subsets: correct and faulty. Each correct entity presents one legitimate identity to other entities of the distributed system. Each faulty entity presents one legitimate identity and one or more counterfeit identities to the other entities. Each identity is an informational abstract representation of an entity that persists across multiple communication events. The entities communicate through messages. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt a distributed computing application that relies on redundancy by injecting false data or suppressing critical data it is sybil attack.

There are various types of tracing mechanisms against sybil attack: trusted explicit and implicit certification, robust authentication, resource testing and incentive based game. In case of trusted certification, a centralized authority assigns a unique identity to each entity. The centralized authority verifies computing, storage and bandwidth capability of the entities associated with the broadcasting system on periodic basis. The recipients validate the received data from the sender and checks logically whether there is any inconsistency or chance of injection of false data in the decrypted message. Another approach of tracing is to adopt incentive based game wherein the objective of the detective is to compute the optimum possible reward that reveals the identity of maximum number of corrupted agents. A local identity (l) accepts the identity (i) of an entity (e) if e presents i successfully to l. An entity may validate the identity of another identity through a trusted agency or other entities or by itself directly. In the absence of a trusted authority, an entity may directly validate the identities of other entities or it may accept identities vouched by other accepted entities. The system must ensure that distinct identities refer to distinct entities. An entity can validate the identity of other entities directly through the verification of communication, storage and computation capabilities. In case of indirect identity validation, an entity may validate a set of identities which have been verified by a sufficient count of other identities that it has already accepted.

(*Case-1.6 : E-healthcare*): E-health is a significant development of the use of emerging information and communication technologies i.e. internet in the healthcare environment. E-health while promising also presents new business challenges in terms of acceptable standards, choice of technologies, overcoming

traditional jurisdictional boundaries, upfront investment, privacy and confidentiality. New and evolving information and communication technologies are being adopted by healthcare sector worldwide. It is becoming a commonplace for healthcare systems to deploy an e-healthcare architecture that consists of extranet, intranet and the internet to create a seamless access to data across a set of distributed healthcare systems.

E-healthcare is able to promote bio-terrorism intelligently through many ways. The content of medical and healthcare websites must be carefully designed and audited to resist false data injection attack on the details of drugs, medicine, treatment procedure, doses and side effects. It may not be possible for the common public to treat their ailments just through web search. Clinical decision making is a complex and multi-dimensional problem which needs specialized skill, training and experience of the healthcare consultants. An website should provide detailed information on the availability of healthcare institutes, consultants, distribution and retail outlets and offered healthcare services to the common people correctly. But, it is risky to give detailed data on medical treatment procedure which may confuse the public to take correct clinical decisions.

The model checking algorithms must verify a set of critical parameters such as the risk of snooping and phishing, validation of service oriented computing schema in terms of logic, main flow, sub flows and exception flows of the application, cross site scripting, injection flaws, malicious file injection by testing application programming interfaces and code, insecure direct object reference, cross site request forgery, information leakage and improper error handling, broken authentication and session hijack, insecure cryptographic storage and failure to restrict URL access.

Secure service oriented computing should protect the users from various types of malicious attacks. *Phishing* is the misrepresentation of a web link where the malicious agents use social engineering to appear as a trusted identity. They leverage the trust of the users to gain vulnerable information via web link, e-mail or instant messages. The phishers try to capture usernames, passwords and other private information of the users by attacking social web sites, auction sites and online payment processors and cause damages ranging from denial of service to financial loss. There are different types of phishing techniques such as link manipulation, filter evasion, website forgery and cross site scripting. The common resolution techniques are user training and the security measures to be embedded in SOC. The users should be able to recognize phishing attempts and should follow privacy and security policies and license agreements. Anti-phishing measures should be embedded in browsers and website login procedures. The website should be authenticated such a way that it indicates that the connection is in authenticated mode and confirms the authenticity and correctness of the particular site to the user.

In case of *cross site scripting [XSS]*, the attacker executes malicious script in the browser of a user and may hijack the session of the user, deface web site and introduce worms. XSS flaws occur whenever an application takes the data from the user and sends it to a web browser without validating or encoding the content. Preventing XSS requires a secure architectural approach such as input validation,

strong output encoding and monitoring of canonicalization errors on a regular basis. The system should validate the configured business rules and reject invalid inputs. The data supplied by the users should be appropriately entity encoded. The inputs must be decoded and canonicalized to the internal representation of the application before proper validation. *Cross site request forgery* attack forces the browser of an active user to send a pre-authenticated request to an web application and forces the victim's browser to perform a malicious action for the benefit of the attacker. The system should not rely on the credentials or tokens being automatically submitted by the browsers. Reauthentication of sensitive data is required to verify a genuine request.

SQL, HTML and XML *injection flaws* occur when an interpreter receives the data from a user as a part of a command or query; the malicious data force the interpreter to execute unintended commands and the attackers can create, read, edit or delete any data. SOC should support a standard input validation mechanism, strongly typed parameterized query application programming interfaces and object relational mapping libraries. The application should avoid dynamic query interfaces and simple escaping functions and should monitor canonicalization errors. Malicious file execution allows the attackers to perform remote code execution, remote root kit installation and total system compromise. SOC should use an indirect object reference map and strongly validate user's inputs. The firewall rules should prevent the web servers making new connections to external web sites and internal systems. Insecure direct object reference occurs when a developer exposes a reference to an internal object like file, directory, database record or key. The attackers can manipulate those references to access other objects without authorization. SOC should not expose private object references to the users, validate any private object reference and verify authorization to all reference objects.

A service oriented application should not disclose their configuration and private functions through error message, debugging and path information or other means. This requires an efficient exception handling approach. The other critical issues are broken authentication, session management and insecure cryptographic storage. Proper authentication and session management is critical to secure service oriented computing. Account credentials and session tokens should be properly protected so that the attackers can not compromise passwords or keys or to assume the identities of the users. Secure SOC should properly authenticate the users and protect their identities and associated credentials. Attackers may use weakly protected data to conduct identity theft. The application should encrypt sensitive information in a data warehouse. The link of a web application should not be disclosed to the unauthorized users. Proper access control should be enforced in the presentation layer and the business logic for all URLs in the application.

Theorem : Life-science supply chain is a soft target of bio-terrorism. The drugs and medicines sold through popular distribution channels may be tainted, compromised and mislabeled. It needs strong support of drug quality and security act.

The life-science supply chain has developed and produced breakthrough drugs and medicines that enhance the average life span in the world. Unfortunately, when bad

things happen in life-science supply chain, the public get hurt. Product recalls are often seen in life-science supply chain. During November 27–December 31, 2013, there were eight recalls by FDA in USA. Today's life science supply chain requires an effective 'Drug Quality and Security Act and Standards' which is able to clarify with transparency the authority, roles and responsibilities of food and drugs administration and consumer protection ministry, regulate pricing of drugs, develop a national track-and-trace system to audit the functions of the life-science supply chain and minimize the risks of contamination, adulteration, diversion or counterfeiting.

A complex life-science supply chain is a network of firms that satisfies the demand of the customers for healthcare products and medical services. The basic objective is to improve the quality of service in patient care by integrating different business units through systematic coordination of material, information and financial flows. In the context of bio-terrorism, the target points of a complex multi-tier life-science supply chain are SCOR, DCOR and CCOR. SCOR includes supply chain planning in terms of demand forecasting, inventory control, production and capacity planning, packaging and labeling, materials requirement planning (MRP); supply chain collaboration and sourcing; supply chain execution through sales and distribution planning, order management, warehouse management, transportation management and reverse logistics. DCOR includes innovation, product life-cycle management (PLM) and pricing and CCOR includes customer relationship management. A malicious agent is able to launch attacks on a life-science supply chain through these channels. The following cases support the reasoning of the theorem.

(*SCOR Case-3.1 : Corrupted Packaging and Labeling*) : Misleading and confusing content, statistical jugglery and data mining on packaging and label of medicines and drugs distributed through consultants, retailers, wholesalers, distributors and other common channels : It is observed on various products such as (a) hair care products, (b) nutritional food supplement i.e. multi-vitamin, multi-minerals tablets. This is a fundamental problem of supply chain management of life-science products. Herbal and Unani drugs are sold at high price in retail outlets in the camouflage of allopathic medicine.

(a) Drug X: It is prescribed to the aged patients as a multi-vitamin, multi-minerals capsule. The detailed data on ingredients are not clearly mentioned on dark red colored label and packet of drug X. Who is verifying and validating the authenticity of ingredients and chemical compositions of drug X? The consumers suffer from constipation and gastric problem after regular use of drug X. They have become suspicious about the side-effects and authenticity of the drug. There may be cascading side-effects due to the use of various drugs on human body and mind. For example; drug X causes side-effect as gastric and constipation problem; Drug Z is used to resist this side-effect and causes another side effect of ulcer.

(b) Drug Y: On its packet, the ingredients are mentioned as Zinc Sulphate Monohydrate, Copper Sulphate Pentahydrate, Borage oil, Gamma Linolenic acid, Selenium and others. Are these elements good for human health? Do they have radioactive effect or any other side effects on human cell? It is not clearly mentioned

whether this medicine can be used for hair care though the picture of hair of a young man is shown on the packet. It is also confusingly stated that the product is not intended to diagnose, treat, cure or prevent of any disease and the product is proprietary food dietary supplement not for medicinal use. It is also mentioned not to exceed the stated recommended daily dose. But, the dermatologists and hair care specialist prescribe the product for hair care treatment. Why the label is not clearly informing that it is a hair care product or a product suitable for chemotherapy treatment; who should not use the products; what are the adverse side effects of the use of the medicine? The information should be transparent and accountable and also trust worthy. There is no short pamphlet or product brochure in the packet of drug Y. Both drugs X and Y have color such as orange and light blue. When the tablets are put in normal water, colors are mixing with water. Are these color pigments enhancing the risk of cancer of the consumers?

(*SCOR Case-3.2 : Corrupted Sales and Distribution System*) : This is the case of corrupted sales and distribution system of toxic and tasty junk food and beverages in the open market. The public including the children regularly suffer from the sale of junk food in the open market such as banana chips, spicy biriyani, masala paste, mughlai roll and cutlet, herbal drugs, country liquor, noodles, pasta, colored soft drinks, colored sweets, chocolates, pickle, tobacco products (e.g. gutkha, biri) and fast food and snack items and often affected with cancer, stomach kidney and liver upset and digestions problems due to the presence of artificial preservatives, color and flavor. In an industrial town, it is often seen the association of a meat slaughter shop (e.g. chicken, mutton, fish), non-vegetarian food outlet (e.g. biriyani) and liquor shop side by side. The poor and uneducated laborers of factories consume such junk food and beverage and suffer from hepatitis, jaundice, liver and pancreatic cancer and die prematurely. There is no action from consumer protection department to ban the sales and distribution of these malicious elements in open market. Fraudulent advertisements of cosmetics and creams are often broadcasted on beauty care products; are they really effective? There should be more focus on the nutrition of the children, boys, girls and the youth of the world for their proper health and development of body and mind through yoga, meditation, sports and games. They should be able to lead a good life-style and stress free life. Price inflation of essential food and beverage items often cause malnutrition of the poor people. Nutrition, education, adoption of best healthcare practices, sustainable development programs, common sense on maternity and childcare are very important for an innovative healthcare programme management. What is the responsibility of SD module of ERP system in life-science supply chain management? The solution is strict regulatory compliance imposed by sensible and responsible corporate governance.

(*SCOR Case-3.3 : Flawed Inventory Planning*): Inventory management is a critical challenge in life science supply chain due to uncertainty of demand and short time interval between manufacturing date and expiry date. The healthcare consultants are often pressurized by the sales people of life-science firms to push new or slow moving drugs, medicines and bio-medical devices of old models for the use of service

consumers. Today, the healthcare consultants often prescribe drugs and medicines based on the availability of stock in the retail outlet. Analytics should be intelligently used for efficient inventory management to monitor dead stock, slow moving stock, ABC analysis and XYZ analysis. It is essential to minimize the wastage of blood and donated organs through improved storage system. Intelligent heuristics should be used to reduce overstock or stock out situation. Example: EOQ = Forecasted demand + Safety stock – Pending order – Current stock. The overstock should be distributed to the poor and needy people in time through efficient distribution planning. The basic objective is to attain approximately zero wastage.

(*DCOR Case-3.4 : Inhuman PLM*): Product life-cycle management (PLM) is a critical part of life-science supply chain. The concept of threshold heuristics is maliciously adopted to limit the life-cyle of senior citizens as a part of artificially intelligent public health and inhuman economic policy in many developing countries. For example, if an old man is above 75 years old; he will be ill treated in hospitals hook-or-by-cook to ensure death through modern killing machines. Basically, it violates the fundamental human rights of living. Still today, effective medicines, drugs, biomedical devices, surgical operations and treatment procedure are not discovered for different life-threatening ailments such as diabetes, cancer, cancer of mind, migraine and headache rheumatic arthritis, joint and knee pain and orthopedic problems of aged people. In case of diabetes, there is no permanent solution for recovery. A diabetic patient is forced to take medicines continuously for blood sugar control within safe limit. If he / she stops medication, the blood sugar will be out of control. This is the failure of modern medical science. The life-science supply chain needs innovation in product life-cycle management on drugs, bio-medical devices and medical practice.

E-health is a promising IT platform of healthcare services. An efficient information system integrates various enterprise applications such as life-science supply chain and healthcare service chain while maintaining individual autonomy and self-governance. The system should support confidentiality, message integrity, non-repudiation, auditing and availability of service in time. The system should support sharing of data in a collaborative business environment wherein a group of trading agents can exchange strategic business information maintaining the privacy of critical data. Increased organizational agility is required for the cooperation of adaptive enterprises. Information technology can improve the quality of service and reduce cost in healthcare services. The demand for critical patient care is growing. But, many small rural healthcare centers are facing problems to develop and maintain a costly IT infrastructure. This forces those healthcare centers to search for innovative IT platform. A life-science supply chain can be protected from threats of disruption through intelligent coordination mechanisms, intelligent contracts, multi-party negotiation, economic modeling, buyer-seller behavior, security and privacy of the trading agents, payment determination, dynamic pricing strategy and information flow. E-health provides different types of benefits in terms of greater geographical reach, global sourcing, reduced transaction costs, improved customer service, accuracy, ease of processing, increased productivity and quick access to information.

Theorem 4*: *Healthcare service chain is another soft target of bio-terrorism.

The critical processes associated with a healthcare service chain are registration, consulting, testing, surgical operations, billing, payment processing and follow-up. Generally, different types of information systems are commonly used to support these processes: transaction processing system (TPS), decision support system (DSS), group decision support system (GDSS), knowledge management system (KMS) and business intelligence (BI) system. The primary objective of these information systems is to ensure fairness and correctness in computation of registration card, appointment slip for consulting, prescription by consultant, surgery schedule, quality control certificate, medical test report, discharge certificate, bills and payment receipt, feedback form and patient's guide. The other important issue is to preserve the privacy of patient's personal and medical data. There may be the risks of failure of secure multi-party computation due to following reasons:

(Case-4.1) Incorrect data provided by the service consumers or patients to the registration associate during registration intentionally or due to lack of knowledge or incorrect perception of the patients or their attendants; the patients or their attendants may be irrational in information sharing properly with the service providers.

(Case-4.2) No verification of patient's identity correctly during registration; the cases of emergency situation or accidents may skip verification due to unavailability of data about the patients.

(Case-4.3) Wrong entry of data into various information systems by the healthcare associates due to time and resource constraints or misunderstanding or lack of validation of input data.

(Case-4.4) Computational errors due to wrong configuration of enterprise applications and / or errors in the heuristics, algorithms and quantitative models and / or no updating of data (e.g. service charge, tariff of testing, price of drugs and healthcare products; low accuracy of pattern recognition algorithms in image processing system may result incorrect medical diagnosis.

(Case-4.5) Access control problem causing dangerous errors in information system; a malicious agent may enter false data into HIS during the absence of authorized users.

(Case-4.6 : Testing) Swap or mixing of test data of various patients or drugs administration due to confusion, poor document management, lack of clear understanding or training of the healthcare workforce; false data injection on viruses in test reports are serious threats in today's healthcare practice. The patients are not often given test reports today by the service provider to hide malicious trading practice or to charge extra amount. Testing of uncommon viruses (e.g. Dengu) enhance the cost of testing unnecessarily. Sometimes, broadcast of epidemic results panic among the public and this critical and helpless situation is exploited by malicious testing and medicare practice inhumanly.

(Case-4.7) Errors in decision making by the health consultants due to lack of proper knowledge management system (e.g. case based reasoning, intelligent DSS and GDSS) or misperception or lack of coordination among the workforce of various

departments or inappropriate enterprise application integration or error in test reports; incomplete prescription due to memory failure or silly mistakes.

(Case-4.8) Errors in scheduling due to exceptions (e.g. unfit patients, non-availability of healthcare experts), flawed and inadequate doctor-patient ratio;.

(Case-4.9) surgical operation by unauthorized and unskilled workforce, intentional errors due to malicious business practice, lack of ethics, casual approach and dull HR policy; unintentional errors due to physical and mental fatigue for excessive workload and sickness, nonavailability of basic infrastructure and logistics arrangements;

(Case-4.10) Lack of verification of correctness of computation in medical billing and payment processing by the service provider and / or service consumer;

(Case-4.11) Incorrect data in patient's help guide may cause confusions and mismatch between the computed results and perceived one;

(Case-4.12) Incorrect feedback by the patients or their attendants due to misperception, misunderstanding of feedback form, lack of knowledge and critical observations or casual attitude.

A malicious agent may launch attacks on TPS, DSS, GDSS, KMS and BIS through malicious data mining, insecure data storage, flaws in data visualization and image processing algorithms and transaction processing logic. A secure service oriented computing model must address correct identification, authentication, authorization, privacy and audit for each e-transaction. For any secure service, the system should ask the identity and authentication of one or more agents involved in a communication. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After the identification and authentication, a service should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of his scope. The system should ask the credentials of the requester; validate his credentials and authorize the user to perform a specific task. Each trading agent should be assigned an explicit set of access rights according to his role. Privacy is another important issue. A trading agent can view only the information according to his authorized access rights. Finally, the system should audit each transaction - what has happened after the execution of a specific service.

Today, healthcare faces critical legal, ethical and psychological issues from the perspectives of security, privacy, confidentiality and organizational policy. Security and privacy of data is important from the perspectives of access control, data storage, version control of critical applications, accountability, traceability and transparency E-healthcare information should be managed in a digital environment through efficient security principles, privacy laws and policies in the domain of shared and managed care. Shared care is a healthcare service that is delivered at multiple locations and by multiple service providers through sharing of the medical information of the patients. Managed care is characterized by cost reduction and quality enhancement techniques practiced by either healthcare service providers or insurance companies. Both paradigms require secure exchange of patient's private data through internet. Another important issue is effective implementation of

Hospital Protection Act in the event of the death of the patients and the arrest prevention act of healthcare professionals.

Theorem 5: Malicious business intelligence is a critical threat factor of bio-terrorism. The conflict between security intelligence and business intelligence is inevitable. It needs fair, rational and intelligent business model innovation.
Malicious business intelligence attacks a life-science supply chain and healthcare service chain through greedy heuristics in payment function for revenue and profit optimization, economic pressure and incentive policy, fraudulent health insurance model, flaws in investment decision on technology management, irrational and dull HR policy in talent management and chaotics in formulation of public policy, mechanisms and corporate governance. In fact, the conflict between business intelligence and security intelligence is inevitable. It is a disguised form of capital punishment. The properties of secure multi-party computation are applicable to resolve this conflict between security and business intelligence.

(*Case-5.1: Pressure on profit and revenue target*): A critical patient Alice is treated in intensive care unit unnecessarily for long duration even there is no hope of recovery. AC charge is billed even after her death. There is another instance of a patient Bob having a simple medical problem. But, he is prescribed costly medical drugs and is treated through different costly testing procedures (e.g. CT Scan, USG, MRI scan) unnecessarily to enhance the cost of treatment. The basic objective is to maximize the revenue from medical bills. There are various models: A healthcare consultant takes high service charge; correctly diagnose and recommend optimal drugs and testing procedure. The consulting charge is high, but the treatment cost is reasonable. In another model, the consulting charge is minimal, but the cost of treatment such as the cost of testing and medicine is very high. Which is really a good model?

(*Case-5.2 : Fraudulent Health Insurance Products*) : This is the case of a people-friedly affordable health insurance model. Health is wealth. But, life is full of uncertainties. The cost of healthcare is rising but the earning is getting low. In this situation, the people are forced to drain all their savings to pay hospital bills. They can get high quality of healthcare service and tax benefits through a set of intelligent health insurance plans.
A health insurance plan should cover hospitalization expenses including consulting testing and surgical operations, ambulance, room rent, boarding and nursing expenses. Thus, the common people can avail financial security, high quality of healthcare service and tax benefits. But, they should be rational in buying appropriate health insurance plans considering various terms and conditions, scope, needs and budget. Generally, health insurance is a yearly policy which should be renewed each year subject to certain exclusions and waiting period. Health insurance can be claimed in two ways: reimbursement and cashless. In case of reimbursement, a person gets admitted in a hospital, pays hospital bills, submit the documents and claim form to the insurance service provider for reimbursement. On the other side, a health insurance service provider may have a network of hospitals

with specific arrangement for direct billing. An insurance person is admitted in a network hospital by submitting a cashless card. The hospital processes cashless admission of the patient and hospital expenses are paid by the insurance service provider covered by the plan.

The financial intelligence of healthcare service is associated with multiple payment processing options such as health insurance, credit card, direct cash payment, bank loan and donation. Another important issue is discriminatory pricing of drugs, biomedical devices, helathcare and surgical products and services and also combinatorial pricing plan for different packages. The basic building block of digital transformation is a well-designed web application schema. The content of the web portal should be defined intelligently and is expected to provide a transparent overview of various types of health insurance plans, their benfits and limitations, business rules, group buying strategy, cliam processes (reimbursement and cashless), payment processing options and discriminatory singular or combinatorial pricing strategy. An online premium calculator should be able to compute premium and service tax for a selected health insurance product, age band and sum insured with a comprehensive cost-benefit analysis, risk assessment and mitigation strategies and tax savings. The service consumers and health insurance service providers should be able to process buy, renew, claim and reimburse functions online maintaining privacy, fairness, correctness, trust, transparency and rational information exchange. Additionally, the web enabled application should provide detailed information on help guide, buying tips, free helpline number, mobile commerce model, customer service contact number and e-mail id, legal and regulatory compliance issues correctly.The payment function should be designed innovatively, fairly and rationally in terms of intelligent contract, pricing strategy, payment terms, incentives and penalty function. It is essential to audit malicious business intelligence of a health insurance model by verifying transparency and accountability of the payment mechanism from the perspectives of violation in contractual clauses among the agents, flaws in payment function computation or pricing algorithm and package configuration and commitment.

(*Case-5.3: Malicious HR Policy for Talent Management*) For effective healthcare system innovization, digital technology management is not only the critical success factor. There are other several factors such as HR policy in talent management, quality of medical education, intelligent public policy, mechanisms and corporate governance. The healthcare consultants, specialists and work force need a good human resource management model for proper talent acquisition and retention, research and innovation, career growth planning, incentive, reward, recognition and retirement planning. The healthcare service provider may have a flawed business model based on old legacy information technology, malicious healthcare practice due to economic and financial pressure, mechanical HR policy and bad resource allocation mechanism. The patients or service consumers may lose trust in health care products and practice due to costly treatment procedure, complicated and fraudulent business rules and vague computational intelligence. Such an inefficient system increases the risk of bio-terrorism through malicious behavior of the trading agents, administrative inefficiencies, collusion of the trading agents

against regulatory compliance, financial fraud in e-transactions, quality problems in testing and sourcing, non-availability, poor performance and failure of medical equipments, malicious work culture, medical negligence, unauthorized absence, excessive work load, strikes and physical security problem of healthcare service provider. The healthcare workforce expect to work freely in a collaborative, flexible and ethical work culture without any financial, physical, mental and cultural constraints and pressures.

Globally healthcare organizations are undertaking massive business process reengineering initiatives and many of these reforms are supported by the strategic use of advanced information and communication technology. It should provide better integration and improved coordination of flows of material, information and funds within and across healthcare firms, experts and patients. This results improved patient care, greater accuracy, cost efficiency, ease of processing, increased productivity and fast response time in healthcare service. Service oriented computing results improved interoperability, increased federation, and organizational agility through a standardized, flexible, reliable and scalable architecture. However, it enhances the risk of various types of malicious attacks on the healthcare service chain and life-science supply chain and these are the emerging threats of bio-terrorism today.

Cryptographic challenges

Theorem : It is essential to develop new cryptographic tools and techniques to satisfy multi-dimensional properties of secure multi-party computation for ensuring security intelligence of a complex system at improved cost of computation and communication.

Traditionally, the concept of encryption and decryption has been used to preserve the privacy of critical data for an intelligent healthcare information system. It is used for private communication and secure data storage. Intelligent transaction processing systems have used cryptographic techniques effectively to ensure authentication, authorization, access control, correct identification, privacy and audit of electronic transactions.The most critical issue is the cost of computation of security algorithms. In the context of secure communication, cryptography ensures privacy and secrecy of sensitive data through encryption method. S encrypts a message (m) with encryption key and sends the cipher text (c) to the recipients (R). R transforms c into m by decryption using secret decryption key. An adversary may get c but cannot derive any information. R should be able to check whether m is modified during transmission. R should be able to verify the origin of m. S should not be able to deny the communication of m. There are two types of key based algorithms: symmetric and public key. Symmetric key encryption scheme provides secure communication for a pair of communication partners; the sender and the receiver agree on a key k which should be kept secret. In most cases, the encryption and decryption keys are same. Secure authentication is hard with symmetric encryption key with untrusted recipients. In case of asymmetric or public-key algorithms, the key used for encryption (public key) is different from the key used for decryption (private key). The decryption key cannot be calculated from the

encryption key at least in any reasonable amount of time. Asymmetric RSA encryption achieves authentication where each recipient can verify the authenticity of received data but can not generate authentic messages.

A *digital signature* is a cryptographic primitive by which a sender (S) can electronically sign a message and the receiver (R) can verify the signature electronically [36]. S informs his public key to R and owns a private key. S signs a message with its private key. R uses the public key of S to prove that the message is signed by S. The digital signature can verify the authenticity of S as the sender of the message. A digital signature needs a public key system. A cryptosystem uses the private and public key of R. But, a digital signature uses the private and public key of S. A digital signature scheme consists of various attributes such as a plaintext message space, a signature space, a signing key space, an efficient key generation algorithm, an efficient signing algorithm and an efficient verification algorithm. Digital signature provides authentication and non-repudiation through asymmetric property of cryptography at high cost of computation and communication. One way hash function may be used as the basic building block of asymmetric RSA digital signature and cryptographic commitment. A one-way function is a function that is easy to compute but computationally infeasible to invert. If x is a random string of length k bits and F is a one-way function then *F* can be computed in polynomial time as y = F(x) but it is almost always computationally infeasible to find x' such that F(x') = *y*. Merkle hash tree is an efficient construction of one way function.

Another alternative interesting option for secure authentication is *signcryption*. Traditional signature-then-encryption is a two step approach. At the sending end, the sender signs the message using a digital signature and then encrypts the message. The receiver decrypts the cipher text and verifies the signature. The cost for delivering a message is the sum of the cost of digital signature and the cost of encryption. Signcryption is a public key primitive that fulfills the functions of digital signature and public key encryption in a logically single step and the cost of delivering a signcrypted message is significantly less than the cost of signature-then-encryption approach. A system is vulnerable to insecure communication. The basic objective is that the system properly signcrypts all sensitive data. A pair of polynomial time algorithms (S,U) are involved in signcryption scheme where S is called signcryption algorithm and U is unsigncryption algorithm. The algorithm S signcrypts a message m and outputs a signcrypted text c. The algorithm U unsigncrypts c and recovers the message unambiguously. (S,U) fulfill simultaneously the properties of a secure encryption scheme and a digital signature scheme in terms of confidentiality, unforgeability and non-repudiation. *Signcryption* can ensure efficient secure communication. In a triplet Elgamal signature scheme [r,e,s], the commitment r is computed as r = g^k[mod p] where g and p are part of the public key and the commitment k is an integer independent to such values [15]. The signature generation scheme permits the receiver to recover the commitment by computing r = $g^s y^e$(mod p). The sender computes the commitment in such a way that it is only recoverable by the receiver. The commitment value can be used as a symmetric key shared between the sender and the receiver and this symmetric encryption provides message confidentiality. The recoverable commitment value of Elgamal triplet

signature scheme is used as the symmetric key to achieve symmetric encryption of the message while the triplet signature serves the signature.

Alternatively, the agents may adopt different types of privacy preserving data mining (PPDM) strategies such as randomization, summarization, aggregation, generalization, suppression, de-identification and k-anonymity. Intelligent PPDM strategies may improve the cost of computation in secure communication. The basic objective is to provide confidentiality, data integrity, authentication and non-repudiation in the communication of sensitive data.

Let us now conclude this work. The threat analytics clearly shows cryptographic challenges of secure multi-party computation for intelligent and complex systems and critical applications. It is essential to develop new cryptographic techniques and tools which should be able to provide collective security intelligence in terms of correctness, fairness, rationality, trust, transparency, accountability, reliability, confidentiality, data integrity, non-repudiation, authentication, authorization, correct identification, privacy, safety and audit of complex information systems used in healthcare service chain and life-science supply chain. It is essential to detect malicious attacks on the information system and communication schema intelligently in time through efficient model checking and system verification mechanisms. Another critical agenda is to improve the cost of computation and communication of secure multi-party computation protocols. Efficient signcryption and unsigncryption algorithms should be implemented practically in the form of information security solutions. The properties of secure multi-party computation are useful to resolve the conflicts between the security intelligence and business intelligence of a complex mechanism. It is an interesting option to explore the application of secure multi-party computation for the design of intelligent mechanisms through the cross fertilization of cryptography and algorithmic game theory. Is it possible to generate signcrypted e-prescription by healthcare consultants?

6. STRATEGY

Strategy Analytics

***Agents*: system analysts, business analysts, scientist, engineers, technology management consultants;**

***Strategic moves* : Focus on emerging healthcare, life science, biotechnology, pharmaceutical technologies.**

- **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements – scope, system, structure, security, strategy, staff-resources, skill-style-support;**
- **Define a set of security goals and emerging technologies accordingly.**
- **Do SWOT analysis: strength, weakness, opportunities and threats of existing technologies as compared to emerging technologies;**
    - **Fair and rational business model innovation**
    - **Who are the consumers**?

    - What should be the offering of products and services?
    - What do the consumers value?
    - How to deliver values to the consumers at rational cost?
- Do technology life-cycle analysis on ‘S’ curve : presently at emergence phase of ‘S’ curve.
- Explore technology innovation-adoption-diffusion strategy.
    - Cancer prevention strategies
    - Proactive approach
    - Reactive approach
    - Deep learning
    - Intelligent reasoning
        - Case based reasoning
        - Perception common sense reasoning
    - Regenerative medicine
    - Precision medicine
    - Cancer genomics
    - Biomedical technology
- Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.
- Adopt ‘4E’ approach: envision, explore, exercise and extend.

Dr. Muller and Dr. Nil Harvey are analyzing the strategy of innovation, adoption and diffusion of emerging healthcare technologies; it can be analyzed from different dimensions such as proactive self-healing approach, reactive approach, deep learning algorithm, intelligent reasoning and biomedical instrumentation. Intelligent reasoning should be explored in terms of case based reasoning, perception and common sense, logical and analytical reasoning and rational payment function. It is essential to adopt a set of reactive strategies such as alternative, integrated, regenerative and precision medicines to fight against cancer. It is rational to evaluate strength, weakness, opportunities and threats for various strategic options. The evolution and diffusion of cancer prevention technology depends on R&D policy, organization learning, knowledge management strategy and technology life-cycle analysis. An intelligent R&D policy should be explored through shared vision, goal and strategic alliance, collaborative and collective intelligence. There are various strategies of learning such as learning-by-doing and learning-before-doing. Learning-by-doing is effective in cancer care through deep learning on big data; it is also essential to attain deep practical and theoretical knowledge on cancer therapy through experimental medicines. In fact, it is clear from the aforesaid case analysis that different types of cancer demand different types of prediction and prevention technologies, best practices and therapies.

Technology trajectory is the path that the cancer prevention technology takes through its life-cycle from the perspectives of rate of performance improvement, rate of diffusion and rate of adoption in cancer care. It is really complex to analyze the impact of various factors on the trajectory of cancer prevention technology today. From the view of life-cycle, the technology of cancer prevention is at the growth phase of S-curve. The technology has evolved from the birth phase and

going though growth phase. Initially, it may be difficult and costly to improve the performance of the new cancer prevention technology. The performance is expected to improve with better understanding of the fundamental principles and mechanisms of human biological system. Initially, the technology may be costly for the adopters due to various uncertainties and risks. Gradually, it is expected to be adopted by large segments of the market due to reduced cost and risks. The evolution of the technology is passing through a phase of turbulence and uncertainty; various entities are exploring different competing options of cancer care and a dominant therapy is expected to emerge through a consensus and convergence of the best practices. The dominant therapy must consider an optimal set of technological advancements which meet the demand of the cancer patients, cancer care experts, supply chain and design chain in the best possible way.

Let us consider the strategy of surgical operation for cancer care. It is essential to operate hard and soft tissues with proper care, precision, consistency, speed and control. The surgical operation is expected to be minimally invasive, less painful and faster healing. An innovative technological solution and surgical method for cancer care is expected to have higher success rate; lower recurrence rate, more precision, accuracy and effectiveness, less treatment time, faster recovery and healing, unmatched cutting, speed and control with high consistency and reliability, greater precision and control, efficiency and safety, less post operative problems due to minimally invasive procedure preventing damage to nearby tissues and less bruising, numbness and post operative pain, minimal invasion and no scars, simple OPD procedure, better patient experience and thus high credibility and high patient satisfaction. Laser technology is an emerging solution for the aforesaid desired surgical operation in cancer care.

Laser (light amplification by stimulated emission of radiation) is an effective solution as compared to conventional methods. Laser has a specific wavelength; it is focused in a narrow beam and creates a very high intensity light which is used for cutting through tissue in surgical operation. Laser therapy is used to destroy tumors or precancerous growths in skin, cervical, penile, vaginal, vulvar and lung cancer. It may be also used for cancer related to brain, prostate, piles, fissures, fistula and dental problems. Laser therapy can be used in standalone mode or in combination with chemotherapy or radiation therapy. It is used to relieve certain symptoms of cancer such as to remove a tumor blocking trachea or esophagus or colon polyps or stomach. It can also be used to seal nerve endings and to reduce pain after surgical operation and seal lymph vessels to reduce swelling and limit the spread of tumor cells. Laser therapy is given through a flexible endoscope fitted with optical fiber. It is inserted through mouth, nose, anus or vagina. Laser is then precisely focused to remove a tumor.

There are various types of laser therapies such as Laser-induced Interstitial Thermotherapy (LITT) and Photodynamic Therapy (PDT). Generally, CO_2, argon and neodymium: yttrium-aluminum-garnet (Nd:YAG) lasers are used for cancer care. Laser therapy provides several benefits such as minimally invasive procedure, faster recovery, minimal recurrence, blood loss, pain and post operative discomfort and high success rate. Laser therapy demands specialized training of the surgeons

and strict safety precautions. It is expensive; the effects may not last long and may be repeated for recovery.

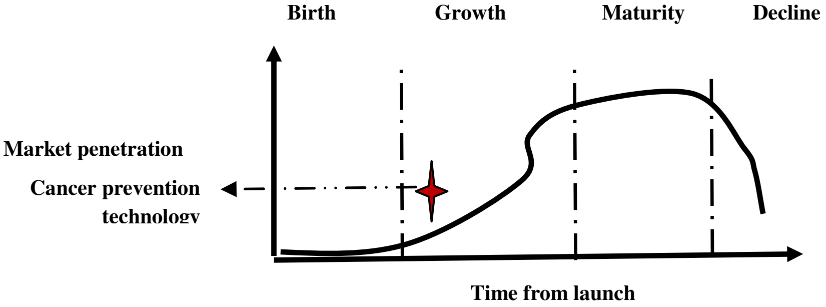


Figure 5.3 : Technology life–cycle analysis

Precision Medicine for Cancer Care : **Let us exercise SWOT analysis on *precision medicine*; it is a a medical model having customization of healthcare practice in terms of medical decisions, treatments, practices, products and services being tailored to individual patient. Diagnostic testing is done for genetic, molecular and cellular analysis to select correct and optimal method of the treatment of a patient using a set of intelligent tools such as molecular diagnostics, imaging, and analytics. Precision medicine is basically tailoring of medical treatment to individual characteristics of each patient; not creation of drugs or medical devices unique to a patient, but rather the ability to classify individuals into subpopulations that differ in their susceptibility to a particular disease or in their response to a specific treatment. Preventive or therapeutic interventions can then be focused on those patients who will benefit considering a set of critical issues such as patient care cost and side effects of medicine. Genomic medicine is an emerging medical discipline that involves using genomic information about an individual as part of their clinical care (e.g. for diagnostic or therapeutic decision making) and the health outcomes and policy implications of that clinical use. P4 is an approach to make medicine more predictive, preventive, personalised and participatory. The basic objectives are to quantify wellness and predict and prevent disease; understand human health and moderate the course of chronic diseases, correct disabling physical conditions and cure molecular deficiencies; it demands the convergence of system medicine, digital technologies and consumer driven healthcare. Personalized medicine is a form of medicine that uses information on genomics i.e. person's genes, proteins and environment to prevent, diagnose and treat disease.**

Precision oncology is the branch of precision medicine for cancer care based on molecular profiling tests and DNA sequencing. Artificial intelligence is providing a paradigm shift towards precision medicine to understand genotypes and phenotypes in existing diseases improve the quality of cost effective patient care and reduce mortality rates. Machine learning algorithms are used for genomic sequence analysis and drawing inferences using big data analytics. Health care service providers are expected to understand better the impact of environment, lifestyle and heredity on patient's health, disease or condition using the knowledge of precision

medicine, They can predict correctly which treatments will be most effective, preventive and safe, There are other several benefits of precision medicine : shift from reaction to prevention, predict susceptibility to disease accurately, improve detection of disease, preempt progression of disease, customize prevention strategies of disease, prescribe more effective drugs, avoid prescribing drugs with predictable side effects, reduce the time, cost, and failure rate of pharmaceutical clinical trials, eliminate trial and error inefficiencies that may inflate health care costs and undermine patient care. One of the critical issues in cancer patient care is the side effects of chemotherapy. Precision medicine may be an interesting strategic move to cure cancer in future.

Cancer Genomics : **Cancer is considered as a *genomic* disease since a normal cell becomes a cancer cell through successive genomic alterations. Molecularly Targeted Agents (MTAs) block a peculiar molecular genomic alteration in cell proliferation, angiogenesis, metastasis and invasion of tumor. Precision medicine analyzes information on genes, proteins, environment, location of tumor and histology of a patient to diagnose, treat and prevent cancer. Precision medicine is an emerging technology in oncology based on the concept of MTAs. It is important to analyze the effectiveness of precision medicine in terms of efficiency of bioinformatics algorithms, histology independent drug development, clinical trials to evaluate a treatment algorithm instead of drug efficacy, molecular genomic alterations across different types of tumor and molecular profiling of tumor of cancer patients.**

RNAs are polymeric molecules which carry genetic information and used in protein synthesis; only a minor fraction of human genomes encode for proteins and the remaining large fraction of the transcripts are noncoding RNAs (ncRNAs). The noncoding RNAs are potential biomarkers and therapeutic targets to facilitate precision medicine in cancer care. It is an interesting research agenda to explore diagnostic, prognostic, biomarkers and therapeutic strategies of ncRNAs. ncRNAs are broadly classified into distinct classes based on the lengths, unique biogenesis routes, three dimensional structure and modes of action such as ribosomal RNAs, transport RNAs, small nucleolar RNAs (snoRNAs), microRNAs (miRNAs), small interfering RNAs (siRNAs), PIWIinteracting RNAs (piRNAs), hairpin RNAs (hpRNAs) and long noncoding RNAs. ncRNAs regulate gene expression through diverse mechanisms such as mediating imprinting, alternative splicing and modification. Deep sequencing technologies generate high throughput transcriptomic and demand the support of efficient bioinformatics mechanisms for proper storage, intelligent analysis, visualization and interpretation of data, RNA identification, structure modeling, functional annotation and network inference. US government invested $215 million to launch Precision Medicine Initiative (PMI) in 2015. It is a customized healthcare model which considers individual variability and tailors medical treatment to individual patient. Precision medicine is dependent on molecular diagnostics to select correct therapies based on genetic data of a patient.

Genomic information is getting used for the diagnosis of lung, breast and pancreatic cancer. The treatment of lung cancer is effective based on diagnostic, prognostic and predictive findings, microRNA profiling and high throughput sequencing. Molecular alterations and routine genomic profiling is getting applied for the

treatment of lung cancer. Evolving technologies (e.g. next generation sequencing, high density microarrays and high throughput expression profiling platforms) enable genomic profiling at a reasonable cost. Pancreatic Ductal Adenocarcinoma (PDAC) is a lethal disease with the worst prognosis among all solid tumors. Genomic landscape has revealed that massive scale sequencing provides unprecedented opportunity to dramatically improve diagnosis and treatment of pancreatic cancer. Breast cancer is the most frequent female cancer. Genomics is effectively used for the treatment of breast cancer through proper hormone therapy.

***Regenerative Medicine for Cancer Care* : The basic objective of *regenerative medicine* is to develop methods for regrowing, repairing or replacing damaged or diseased cells, organs or tissues (William Haseltine,1999). It includes generation and use of therapeutic stem cells therapy, tissue engineering, molecular biology, cell transplantation, production of artificial organs and biomechanics prosthetics. It deals with the process of replacing, engineering or regenerating human or animal cells, tissues or organs to restore or establish normal function. It tries to engineer damaged tissues and organs by stimulating the body's own repair mechanisms to functionally heal previously irreparable tissues or organs. It includes the injection of stem cells obtained through directed differentiation (cell therapies); the induction of regeneration by biologically active molecules administered alone or as a secretion by infused cells (immunomodulation therapy); and transplantation of in vitro grown organs and tissues (tissue engineering). It is relatively a costly treatment. There are various types of regenerative medicine such as Stem cell therapy (Stem cells injected into bone, cartilage or fat cells to stimulate healing in the body), platelet rich plasma (prp), lipogems and prolotherapy. Stem cell injections may last upto one year. Stem cells may be effective in cancer care to repair, restore, replace and regenerate cells at the target location,**

Regenerative medicine covers a range of treatments intended to repair or replace damaged cells, tissues, or organs such as cell therapies, bioengineered tissue products, and gene therapies. Stem cell treatment involves infusion of healthy stem cells into the patient through a painless process of stem cells transplantation through intravenous (IV) infusion. For bone marrow or blood stem cell transplant, engraftment takes 2-3 weeks; for cord blood transplant, it takes 3=5 weeks. Stem cell transplant has some negative side effects such as low blood cell counts, Graft-versus-host disease (GVHD), Veno-occlusive disease (VOD), digestive system problems. skin and hair problems. pain, kidney and lungs problem. The success rate is 82.2%. The basic objective of regenerative medicine is to provide safe and reliable ways to repair, restore or replace damaged tissues or organs. Cord blood and tissues are the building blocks of regenerative medicine. Natural stem cells extracted from embryonic, hematopoietic, mesenchymal or adult tissues) or induced progenitor stem (iPS) cells can be modified by gene therapy for use in regenerative medicine. Stem cell therapy is useful for regrowth of cartilage, knee pain and growth of hair. There are side effects such as temporary swelling and pain. Regenerative medicine is an interesting strategic option of cancer care in future.

***Integrated Medicine for Cancer Care*: *Integrative medicine* may be any type of medical practice or product that is not standard care. For cancer, standard care may be surgery, chemotherapy, radiation and biological therapy. Integrative medicine is complementary care used alongwith standard care. For cancer, it combines the best of both types of care. It is a combination of medical treatments for cancer and complementary therapies to cope with the symptoms and side effects. Complementary Alternative Medicine (CAM) may include acupuncture, yoga and meditation for treatment of cancer and scientific evidence supports this approach to health and healing. Can cancer be cured naturally? There is no evidence of alternatives of cancer cure. Alternative complementary therapies can interfere with chemotherapy or radiation and make them less effective or may have other negative effects. Integrative medicine combines complementary treatments with conventional care. Conventional medicine relies on methods proved to be safe and effective with carefully designed trials and research. But, many complementary and alternative treatments lack solid research for sound decisions. What are the benefits of integrative medicine? It is a comprehensive approach to care i.e. treating the patient through a holistic approach; not just the condition or disease; setting the foundation for overall health, This method may reduce the cost of cancer care. But, it may have negative effects or even risks of death. What is the best treatment for cancer? In fact, cancer care may be done effectively through a combination of treatments such as surgery with chemotherapy and/or radiation therapy, immunotherapy, targeted therapy or hormone therapy, precision medicine, regenerative medicine and integrated medicine.**

Dr. Muller is analyzing the strategy of innovation, adoption and diffusion of biomedical technologies. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision and goal,. Biomedical innovations are closely associated with various strategies of organization learning and knowledge management. The aforesaid biomedical innovation is closely associated with R&D policy and organizational learning strategies in new product development. There are various strategies of learning such as learning by doing and learning before doing. Learning before doing is possible through laboratory experiments, prototype testing and simulation. Deep practical and theoretical knowledge can be achieved through laboratory experiments. Learning by doing is also important to understand the impact or side-effects of the implantation of biomedical devices and oral insulin.

Technology innovation on biomedical technology is associated with various strategic moves and functions such as scope analysis, requirements engineering, quality control, product design, concurrent engineering, talent management, team management and coordination, resources planning, defining products specification, concept development, concept evaluation, system architecture design, detailed design, production plan development, roll out, prototyping, testing, documentation, tools development and regulatory issues [37-38].

The design of a medical product is a complex task having uncertain information, high stakes and conflicts, varieties in size, scope, complexity, importance and cost and various constraints in terms of product quality, product cost, development cost,

development time and development capability. It is essential to adopt concurrent engineering approach which considers all aspects of the problems faced and a clearly defined role. It is challenging to develop a product development team with specific skills and group dynamics. The next step in our process is to transform these needs into specifications that can be used to guide the design decisions. These product specifications become the targets for the product development. The concept development phase is the time to search out ideas that will meet the need. Next important steps are concept evaluation through SWOT analysis, design of system architecture, prototyping and product testing. Finally, it is essential to satisfy various issues of regulatory compliance such as approval of FDA. It is not a simple task to make rational decisions on strategic technologies, ICT, technology infrastructure development and renewal of existing technologies.

***SWOT Analysis*: It is an interesting research agenda to analyze strength, weakness, opportunities and threats of innovation on biomedical technology. Strength indicates positive aspects and benefits; weakness shows negative aspects and limitations of the same; opportunities explore the growth potential and threats assess the risks of the technology. Let us compare two strategic options for the treatment of diabetes: oral insulin vs. artificial pancreas based on biomedical technology. The critical observation from this deep analytics is that oral insulin is a rational, simple, practically feasible and safe option as compared to artificial pancreas. But in case of pancreatic cancer, artificial pancreas may be an essential option. However, the concept of artificial pancreas is a very complex and costly strategic option and there is threat of immunity and safety from the perspectives of adaptability of human biological system. But, both the aforesaid options are not matured at their technology life-cycle; they are now at emergence phase. It is also essential to adopt a set of proactive and reactive measures to fight against diabetes such as herbal and homeopathic medicines, yoga, meditation, healthy life-style, obesity control and organ replacement.**

Diabetes is a disorder of deficiency in insulin, a peptide hormone of pancreas. Insulin is generally given by subcutaneous (SC) route; the non-compliance of diabetic patients is a common occurence. Oral insulin is an alternative option but it is essential to identify appropriate delivery mechanism. Oral insulin is the dream of diabetic patients. Nanotechnology may be an innovative strategic option in this connection due to the size of particles in nano range and greater surface area [3,4]. These physical and chemical properties improve the absorption of nanoparticles as compared to larger carriers. This is a real challenge of today's research on oral insulin from the academic and industrial community. Is it possible to use nanoparticles as a carrier to deliver insulin orally?

Let us analyze the strength and opportunities of oral insulin delivery mechanism which support a cost effective, convenient, simple and painless treatment; it reduces the risk of hypoglycemic incidents, immune responses and obesity. The threat and weaknesses of SC route mechanism may be considered from various aspects such as hyperinsulinemia, lipoatrophy, lipohypertrophy, patient noncompliance, painful procedure of injections and cost for the treatment for hyperglycemia, retinopathy, neuropathy and nephropathy. There are various types of Diabetes Mellitus such as Type I, Type II, gestational and secondary.

Now, let us consider the strength of nanomedicines. For oral insulin delivery, it is possible to explore various types of options such as nanoparticles (NPs), liposomes, microemulsions (MEs), self-nanoemulsifying drug delivery systems (SNEDDS), micelles, nanogels (NGs), microspheres, niosomes, and superporous hydrogels (SPHs). A NP is a small entity, particle size ranges from 10 to 1000 nm. Two major pathways by which NPs pass through intestinal epithelium are paracellular and transcellular. Transcellular route is the most common route of absorption. NPs can be classified into polymeric and lipid-based systems. Biocompatible and biodegradable polymeric NPs may be an ideal carrier for delivering proteins and peptides orally. It improves bioavailability of oral insulin. It may be Nanospheres and nanocapsules. Solid lipid nanoparticles (SLNs) offer some advantages like nano size range and comparatively narrow size distribution, controlled release of drug over a long period of time, protection of drug against chemical degradation, nontoxic, relatively cheaper and stable and can be easily freeze or spray dried. Liposomes offer several advantages such as nanosize, able to incorporate both hydrophilic and hydrophobic drug, improved effectiveness, better stability by encapsulation, non-hazardous, compatible in biological environment, biodegradable, and nonantigenic; biotinylated liposomes (BLPs) enhance the delivery of insulin.

Nanocarrier based systems for mucoadhesive drug delivery systems prevent degradation of entrapped drug and improve the circulation time of drug at absorption site. Polyionic polymers show mucoadhesive properties. From such polymers, alginate has shown the best candidate for the intestinal mucosal system. Alginate is a nontoxic, biodegradable, and mucoadhesive polysaccharide polymer that possesses mucoadhesive properties than carboxymethylcellulose, chitosan, poly (lactic acid), and other polyionic polymers.

It is essential to improve oral insulin delivery mechanism due to incomplete and unpredictable absorption through gastrointestinal tract, degradation due to varying pH of the stomach and enzymatic degradation lead to poor oral bioavailability. The structure of insulin is very delicate. Stability is affected by component and processing elements; the common degradation pathways are oxidation, photodegradation, disulfide scrambling, deamidation, aggregation, precipitation, dissociation and fragmentation.

Next let us focus on strength and weakness of artificial pancreas. Artificial pancreas is a technology that controls blood sugar level of diabetes patients and acts as the substitute of a healthy. A pancreas performs various exocrine digestive and endocrine hormonal functions There are alternative options of treatment such as insulin replacement therapy having life saving capability and manual control of blood sugar level with several limitations. The basic objectives of artificial pancreas is to improve insulin replacement therapy and to ease the burden of therapy. There are various types of approaches such insulin pump through close loop control based on real-time data from a continuous blood glucose sensor, bioengineering approach through surgical implantation of a biocompatible sheet of encapsulated beta cells and gene therapy approach through therapeutic infection by a genetically engineered virus which changes DNA of intestinal cells to insulin producing cells.

Artificial pancreas is used to deliver basal insulin automatically and continuously at meal time by pressing the buttons of insulin pump. Blood sugar data is given to the insulin pump before meals. It calculates the correction bolus to bring the blood glucose level back to the target. But there are several complexities of artificial pancreas such as calibration for sensor correction, correctness in measurement of blood sugar levels, skill, intellect and knowledge of the diabetic patients, maintenance of medical equipments and verification of the correctness of automatic control of basal rate of insulin pump, adaptive filtering for learning unique basal rate, feedback from a continuous blood glucose sensor and adjustment of correction bolus during increase or decrease of blood sugar level. Typically, implantable insulin pumps work for an average of eight years and the sensors stop working after an average of nine months. From the aforesaid analysis, it is clear that oral insulin is a much more simple and rational strategic option as compared to artificial pancreas and demands much more focus of R&D.

It is an interesting research agenda to do SWOT analysis on artificial liver vs. biological liver transplantation. Both the options may be essential for various types of liver diseases such as liver cancer, cirrhosis of liver, jaundice, hepatitis, alcoholic liver problem, chronic liver problem, autoimmune hepatitis, Wilson's disease, black stool, blood vomit, swollen legs and heals and water accumulation. But, there are several constraints such as adaptability and immunity. Can an artificial liver mimic all the functions of a biological liver?

Generally, the patients suffer from liver cirrhosis due to regular consumption of booz; liver cells are destroyed and the liver is scarred due to the effect of alcohol. Non-alcoholic fatty liver disease (NAFLD) is the accumulation of fat in the liver not triggered by alcohol but caused by erratic life-style, high blood sugar, cholesterol and obesity. It often remains undetected and may lead to liver cancer. There are other various types of liver problems such as liver cirrhosis and acute hepatitis [B or C type]. Acute hepatitis are treatable and can be prevented with vaccines but chronic hepatitis or NAFLD are not fully reversible. It can not be cured but can be merely controlled. The common prevention strategies for NAFLD include avoiding fatty food, daily physical exercise, periodic screening of liver and control of blood sugar and cholesterol levels. It is technologically hard to develop an artificial liver that can mimic all the functions of biological liver in human body. Alternatively, it is rational to adopt an optimal mix of proactive and reactive approaches which can protect liver from various toxic effects.

Liver Protection Mechanism:

Proactive approach:

- **Control consumption of booz / country liquor / wine / alcohol for the treatment of cirrhosis of liver;**
- **Avoid excessive consumption of non-vegetarian food (e.g. red meat, egg, fish);**
- **Take fruits regularly (e.g. Jambura or 'batabi lebu', mousambi, orange);**
- **Take herbal medicine periodically and vitamins;**
- **Acute hepatitis are treatable with vaccines;**

- **Avoid fatty food, daily physical exercise, periodic screening of liver and control of blood sugar and cholesterol levels for prevention of NAFLD;**

Reactive approach

- **Acute liver failure: Organ transplantation is a feasible option but it should consider following issues carefully.**
    - **Is there any problem of immunity and infection in case of liver transplantation from other animals?**
    - **Which animal should be considered for organ transplantation: human being, goat, lamb, cow, pig?**
    - **Is it possible to transplant a healthy liver from a dying person to a liver patient?**
    - **Is it possible to set up animal liver bank to preserve animal livers in advance?**
    - **Liver dialysis : BAL can replicate several metabolic functions such as detoxification, lipid and plasma lipoprotein synthesis, carbohydrate homeostasis and production of serum albumin and clotting factors wi9thout using multiple devices. BAL device reduced mortality by about half in acute liver failure cases.**
    - **Is it possible to develop artificial liver that can mimic all the functions of normal and healthy biological liver? It is a promising but challenging task in terms of product design, clinical study and identification of ideal cell source that can grant patients substantial survival benefits compared to standard intensive care.**

Liver transplantation is a feasible solution to acute liver failure but severe shortage of donors is a major constraint. Artificial hepatic support systems should provide optimal cell survival, proliferation and maintenance of sufficient liver functions. Liver is one of the most sophisticated organs in human body, the science of liver tissue construction is also very complex.

The evolution of technological innovation of artificial kidney depends on various factors such as tissue engineering, biocompatible materials, transport mechanism; hemodynamic, absorption, hemodialysis and hemofiltration therapy, animal studies and extensive clinical trials. Can an artificial kidney mimic the metabolic, endocrine, and transport functions of a healthy living kidney efficiently? The present technology cannot replace an ailing kidney with artificial one. It is technically hard and complex to develop artificial kidney and install the same in human body. What are the side-effects of an artificial kidney on human biological system? Is it possible to explore proactive and reactive approaches for the protection of kidneys rationally? Generally, it is recommended to drink water sufficiently and avoid excessive consumption of salts. Is it possible to improve the functions of a kidney artificially using medicines – it may be herbal, allopath or integrated medicine? Dialysis is a popular method of treatment. Acute kidney failure needs organ transplantation and surgical operation. Is there any problem of immunity and infection in case of transplantation of kidney from other animals? Which animal should be considered for organ transplantation? Is it possible to transplant a healthy kidney from a dying person to an ailing patient? These are alternative feasible options as compared to artificial kidney.

It has been possible to simulate the functions of a kidney through renal substitution therapy with hemodialysis or chronic ambulatory peritoneal dialysis (CAPD) and transplant it from a donor to a patient successfully. Dialysis is basically renal substitution rather than renal replacement therapy. It only mimics the filtration function but can not replace homeostatic, regulatory, metabolic and endocrine functions of a healthy kidney. So, dialysis has major medical, social, and economic problems. A biohybrid kidney may have biological and synthetic components. It is expected to offer many benefits such as reduced cost, time and infection and increased flexibility, mobility and life expectancy.

Technological life-cycle analysis **: The basic objective of deep analytics is how to manage evolution of the aforesaid technological innovations effectively. It is really interesting to analyze the impact of various factors and patterns of trajectories of biomedical innovations. It is possible to do the analysis of life-cycle based on S–curve, trajectory, diffusion and dominant design of the aforesaid innovations. Technology trajectory is the path that the new technology follows based on rate of improvement in performance, diffusion and adoption. It is perceived today that the innovations of oral insulin, artificial pancreas, artificial liver and artificial kidney may be at emergence phase of S-curve. On the other side, the innovations on artificial cardiovascular devices and limbs may be at growth phase of the curve. The emergence of such new technologies follow a complex process. It is really hard to understand how the life-cycle of a new technology interacts with other technologies and impacts on healthcare and life-science sectors. The next phase is growth if the technology; initially it is difficult and costly to improve the performance of a new biomedical device. The performance is expected to improve with better understanding of the fundamental principles of the technology and system architecture. Initially, the new technology may be costly and risky for the early adopters. Gradually, it should reduce the cost and risks of the biomedical devices and penetrate the market rapidly.**

The diffusion of biomedical technology and oral insulin depends on how new technologies can spread through potential adopters such as the patients and healthcare consultants. Diabetes is a very common healthcare problem today; the size of the market of oral insulin is expected to be big. The rate of diffusion depends on the effectiveness, reliability, consistency and flexibility in system performance and the economic and demographic profile of the adopters. The rate of improvement of the aforesaid biomedical technology technologies and oral insulin should be faster than the rate of market demand over time; the market penetration is expected to increase with high performance and efficiency of the bio-medical devices and oral insulin. At present, the evolution of these technologies are going through a phase of turbulence and uncertainty; the firms are exploring a set of competing options; a dominant design is expected to emerge through consensus and convergence of biomedical system. The dominant design must consider an optimal set of features which should meet the demand of the patients and healthcare experts in the best possible way.

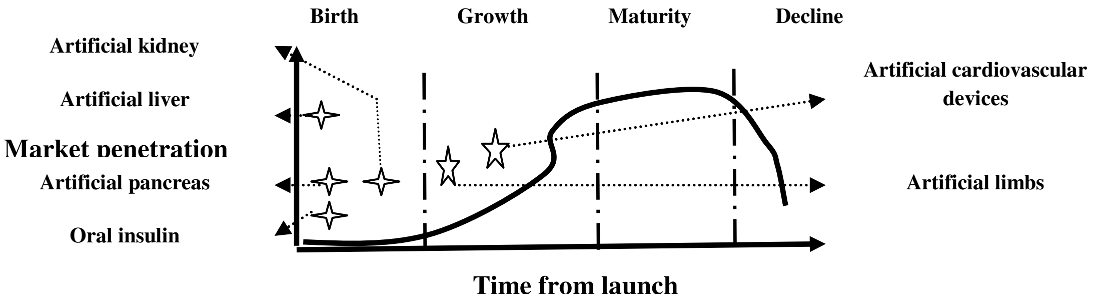


Figure 5.4 : Technology life-cycle analysis

Is it possible to adopt a set of intelligent strategic moves rationally to fight against epidemic and pandemic outbreak globally? The basic objective is to develop an *artificial immune system*. The objective of the strategic moves is not to create any unnecessary panic. Rather, we need a rational, optimal mix of proactive and reactive or adaptive approaches for epidemic control in time. It is essential to formulate an intelligent and rational global security policy as discussed during session 2.

7. STAFF - RESOURCES

Staff-resources Analytics
do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- ***Man*** **: human capital management (scientists, doctors, business analysts, system analysts, project managers, engineers): talent acquisition, talent retention, training, reward and recognition;**
- ***Machine*** **: tools, instruements, computer hardware, software, internet;**
- ***Material*** **: Medicine;**
- ***Method*** **: process innovation for healthcare and cancer care;**
- ***Money*** **: optimal fund allocation, project management, resource allocation and distribution;**

The expert panel have analyzed the demand of staff-resources for healthcare security in terms of sources of innovation and roles of biomedical engineering, pharmacy and life-science firms, oncology departments of healthcare institutes, government research laboratories and collaborative networks; optimal utilization of man, machine, material, method and money, dominant design factors of artificial organs and biomedical devices, process innovation in cancer treatment and technological spillover. The innovation demands the commitment of creative experts of oncology, bio-medical engineering, healthcare and life-science sectors who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs

and activities of R&D lab, start-ups (e.g. science parks, incubators), academic institutions, ministries of state and central government, patients, users and supply chain partners effectively. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision.

The panel are exploring the role of staff-resources for disaster management such as epidemic and pandemic outbreak. The technological innovation on vaccines to fight against new viruses demands the commitment of creative talent from the domains of medical science operations management, management information systems, healthcare administration and biomedical engineering. It is crucial to analyze the dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion, dominant design factors, effects of timing and mode of entry. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment.

It is important to analyze this element in terms of 5M : man (e.g. healthcare staff, nurses, doctors, testing staff, government staff of ministry of healthcare and family welfare, scientists and research staffs of innovation lab), machine (e.g. testing kit, thermal scanner, healthcare infrastructure, camps, hospitals) material (e.g. cleaning agents, sanitizers, masks, gloves, medicine, jacket), method (e.g. process innovation in registration, consulting, testing, broadcasting, governance) and money (e.g. budget allocation for healthcare infrastructure development such as hospitals and quarantine camps, disaster relief fund). 'Man' analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, payment function, compensation, reward, incentive, health insurance of staff and performance evaluation. 'Machine' analyzes the basic aspects of required test kits and medicine of optimal stock. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure. Finally, 'money' highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.

Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. The healthcare institutes and mrdical colleges should define sound research mission and vision and contribute through publication of research papers. Government also plays an active role in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators). Collaboration is facilitated by geographical proximity, regional technology clusters and technology spillovers. Technological spillover results from the spread of knowledge across organizational or regional boundaries; it occurs when the benefits from R&D activities of a firm spill over to other firms.

This is not a trivial problem; it needs useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation,

confidence, commitment and group dynamics. It is difficult to conclude that moderate knowledge is adequate for creativity. A creative person is expected to have confidence in own capabilities, tolerance for ambiguity, interest in solving problems and willingness to overcome obstacles by taking reasonable risks. A cooperative and collaborative environment must recognize and reward creative talent in time. Organizational creativity is associated with several critical factors such as human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routines, incentive policy, social processes and contextual factors.

8. SKILL-STYLE-SUPPORT

Skill-style-support analytics

- ***Skill*: knowledge of operation and best practices of healthcare, life science, bio-technology, pharmacy, technical, system administration, management, governance, supply chain management;**
- ***Style*: leadership, shared vision, goal setting, intelligent communication, risk assessment and mitigation, innovation project management;**
- ***Support* : proactive, preventive and reactive support.**

The expert panel are analyzing skill-style-support for health security. What should be the innovation model for effective diffusion of Cancare ? is it possible to adopt K-A-B-C-D-E-T-F model? The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (e.g. bio-medical engineering, pharmacy, life-science, oncology, deep learning and artificial neural network), healthcare and medical science domain such as research and development, knowledge management, product design, project management, supply chain management, sales and distribution. It is essential to teach deep learning innovatively in various programmes of Electrical, Electronics and Biomedical engineering as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as digital libraries having good collection of books, journals and magazines, software and experimental set up. The workforce of R&D labs can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The healthcare professionals are expected to be people, information and action oriented. Next, let us consider the element support.

Caution from malicious learning system : The basic objective is to protect learning systems in adversarial setting from various types of threats such as use of flawed learning algorithm or intentional change of training and testing data distribution. The malicious agents may act consciously to limit or prevent accurate performance

of the learning system for economic incentives. It is a common problem where machine learning is used to prevent illegal or unsanctioned activities. Traditional techniques (e.g. efficient algorithm, linear classification) are necessary but not sufficient to ensure the security of the machine learning system. It is a hard problem and needs the support of an efficient mechanism equipped with intelligent threat analytics and adaptive secure multi-party computation algorithms. Malicious business intelligence is a critical threat to machine learning system. The conflict between security intelligence and business intelligence is inevitable. It needs fair, rational and intelligent business model innovation.

***Example* : Malicious business intelligence may attack a life-science supply chain and healthcare service chain through greedy heuristics in payment function for revenue and profit optimization, economic pressure and incentive policy, fraudulent health insurance model, flaws in investment decision on technology management, irrational and dull HR policy in talent management and chaotics in formulation of public policy, mechanisms and corporate governance. In fact, the conflict between business intelligence and security intelligence is inevitable; the deep learning mechanism is expected to resolve this conflict between security and business intelligence.**

Let us consider a specific instance of machine learning in healthcare service chain. The deep learning mechanism must call the threat analytics to audit various critical processes associated with a healthcare service chain in cancer care such as registration, consulting, testing, surgical operations, billing, payment processing and follow-up. Generally, different types of information systems are commonly used to support these processes such as transaction processing system (TPS), decision support system (DSS), group decision support system (GDSS), knowledge management system (KMS) and business intelligence (BI) system. The primary objective of these information systems is to ensure fairness and correctness in computation of registration card, appointment slip for consulting, prescription by consultant, surgery schedule, quality control certificate, medical test report, discharge certificate, bills and payment receipt, feedback form and patient's guide. The other important issue is to preserve the privacy of patient's personal and medical data. The deep learning mechanism should verify the security of the computing schema associated with the machine learning system in healthcare service chain to identify probable sources of errors in cancer care.

- **Incorrect data provided by the cancer patients to the registration associate during registration intentionally or due to lack of knowledge or incorrect perception of the patients or their attendants; the patients or their attendants may be irrational in information sharing properly with the service providers.**
- **No verification of patient's identity correctly during registration; the cases of emergency situation or accidents may skip verification due to unavailability of data about the patients.**
- **Wrong entry of data into various information systems by the healthcare associates due to time and resource constraints or misunderstanding or lack of validation of input data.**
- **Computational errors due to wrong configuration of enterprise applications and / or errors in the heuristics, deep learning algorithms and quantitative models**

and / or no updating of data (e.g. service charge, tariff of testing, price of drugs and healthcare products; low accuracy of pattern recognition algorithms in image processing system may result incorrect medical diagnosis.

- **Access control problem causing dangerous errors in information system; a malicious agent may enter false data into HIS during the absence of authorized users.**
- **A malicious agent may launch attacks on TPS, DSS, GDSS, KMS and BIS through malicious data mining, insecure data storage, flaws in data visualization and image processing algorithms and transaction processing logic.**
- **Swap or mixing of test data of various patients or drugs administration due to confusion, poor document management, lack of clear understanding or training of the healthcare workforce; false data injection on viruses in test reports are serious threats in today's healthcare practice. The patients are not often given test reports today by the service provider to hide malicious trading practice or to charge extra amount. Testing of uncommon viruses enhance the cost of testing unnecessarily. Sometimes, broadcast of epidemic results panic among the public and this critical and helpless situation is exploited by malicious testing and medicare practice inhumanly.**
- **Errors in decision making by the health consultants due to lack of proper knowledge management system (e.g. case based reasoning, intelligent DSS and GDSS) or misperception or lack of coordination among the workforce of various departments or inappropriate enterprise application integration or error in test reports; incomplete prescription due to memory failure or silly mistakes.**
- **Errors in scheduling due to exceptions (e.g. unfit patients, non-availability of healthcare experts), flawed and inadequate doctor-patient ratio;.**
- **surgical operation by unauthorized and unskilled workforce, intentional errors due to malicious business practice, lack of ethics, casual approach and dull HR policy; unintentional errors due to physical and mental fatigue for excessive workload and sickness, non-availability of basic infrastructure and logistics arrangements;**
- **Lack of verification of correctness of computation in medical billing and payment processing by the service provider and / or service consumer;**
- **Incorrect data in patient's help guide may cause confusions and mismatch between the computed results and perceived one;**
- **Incorrect feedback by the patients or their attendants due to misperception, misunderstanding of feedback form, lack of knowledge and critical observations or casual attitude.**
- **Sybil attack: It is really complex to trace the corrupted players in healthcare domain. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt an application that relies on redundancy by injecting false data or suppressing critical data; it is *sybil attack*. The patients may be treated incorrectly and diagnosed as cancer casually though there is another simple medical problem. Natural intuition and perception may not be applied for simple medical problems. The patients may be incorrectly recommended for costly treatment. They may be recommended for costly treatment procedure repeatedly (e.g. CT scan, X-ray), drugs and surgical**

operations. The poor and helpless patients may be forced to validate and verify the test reports and medical diagnosis at various healthcare institutes. This is an instance of modern biological, chemical and radiological terrorism today.

Fairness and correctness of computation and testing is a critical concern in cancer therapy. Knowledge management is another critical success factor; case based reasoning may be a good solution for correct clinical decision making. For effective deep learning system, digital technology management is not only the critical success factor (CSF). There are other several CSFs such as HR policy in talent management, motivation and commitment, quality of education in terms of trust, ethics and values, intelligent public policy, mechanisms and corporate governance.

The workforce involved in aforesaid technological innovations are expected to develop different types of skills in technical (e.g. bio-medical engineering, pharmacy, life-science), healthcare and medical science domain such as research and development, knowledge management, product design, project management, supply chain management, sales and distribution. It is essential to teach Biomedical technology innovatively in various programmes of Electrical, Electronics and Biomedical engineering as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented.

It is essential to develop skill in new product development through proper coordination among design, supply and patient chain and R&D, production and marketing functions. The basic objectives are to maximize fit with customer's needs and demands, ensure quality assurance, minimize time to market, and control product development cost. It may be an intelligent initiative to involve the suppliers and the customers in the development process, beta testing, fault tree and failure mode effects analysis and TFPG as part of quality control measures. It is really challenging to manage new product development team through diversity, knowledge base, multiple skills, problem solving capability, cooperative corporate culture and intelligent communication protocol at optimal administrative costs.

Let us analyze skill-style-support. The workforces involved in this technological innovation are expected to develop different types of skills in medical science, immunology, disaster operation management and system administration, innovation on life-science, pharmacy and biotechnology, research and development, testing, tracing, tracking, benchmarked and standardized medical practice. The orkforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and

application of knowledge in a transparent, collaborative and innovative way. The diffusion of the innovation requires the support of great leadership style, effective governance, formation of special task force and expert committee, intelligent and rational corporate communication. The style is basically the quality of leadership; the great leaders must have passion, motivation and commitment. The leaders must be able to share a rational vision, mission and values related to the innovation among all the stakeholders honestly and appropriately in time.

What should be the ideal organization model for this technological innovation? A traditional functionally centered organization model may not be suitable for supporting end-to-end healthcare process. Such process management is more than a way to improve the performance of individual processes; it is a way to operate and manage a business. An enterprise that has institutionalized process management and aligned management systems to support is a process enterprise. It is centered on its customers, managed around its processes and is aligned around a common, customer oriented goal. The business models of top technological innovations require the support of a process enterprise structure enabled with advanced information and communication technology. The structure should have project, design, production, supply chain management maintenance, human resource management, sales & marketing and finance cells. The structure should be governed by an executive committee comprising of CEO and directors. The process managers should be able to identify core processes in the value chain; communicate throughout the organization about these critical processes; create and deploy measures regarding end-to-end process performance and define process owners with end-to-end authority for process design, resource procurement, process monitoring for redesign and improvement. The process enterprise requires a collaborative and cooperative work culture. Innovation in edidemic and pandemic control demands proper technological support in testing and medical diagnosis, proactive, reactive and preventive support for proper technology management. The technology needs the support of a collaborative enterprise model.

9. CONCLUSION

This session has explored the importance of a deep analytics based mechanism for cancer prevention in the context of human biological system. It presents a new framework of human biological system in terms of computing, data, networking, application and security schema of an information system based on analogical reasoning. DACPM promotes a hybrid approach which recognizes the role of both proactive and reactive approaches in making decisions on healthcare investment for cancer prevention. The reactive approach may outperform proactive one against the threats that never occur actually. Sometimes, reactive approach may be cost effective as compared to proactive approach. The basic building blocks of the proposed mechanism are threat analytics and adaptive secure multiparty computation. The threat analytics monitor the system performance of human biological system based on time series data, detects and analyzes different types of vulnerabilities on the biological system.

This work finds a set of interesting research agenda for future work: (a) explore new risk factors and causes of cancer, classifying cancers, opportunities for early detection and prevention and cost reduction of cancer care; (b) how to design an intelligent threat analytics; (c) how to design intelligent verification mechanisms; (d) how to rationalize DACPM, (e) how to quantify and code miscellaneous security intelligence parameters, (e) check the performance of kernel based learning algorithms with CNN, (g) how to apply integrated medicine for critical case (e.g. multiple organ failure syndrome) and exercise allopathic, homeopathy, herbal, yoga and naturopathy effectively for various purposes such as pain management, combating side effects of radiation and chemotherapy (e.g. hair fall, nausea, vomiting), every cancer patient requires specific treatment considering complexity of disease and (g) explore new approaches of cancer prevention such as vaccination for auto-immunity, laser therapy, integrated and regenerative medicine, precision medicine, gene therapy and stem cell therapy and (h) is it possible to imagine the security schema of human biological system based on antivirus, firewalls and various cryptographic tools (e.g. encryption, decryption, digital signature and signcryption) apart from secure multi-party computation? The next session explores the strategic option of bio-medical instrumentation and organ transplantation for various types of cancers such as pancreatic and liver cancer.

The expert panel are summarizing the outcome of deep analytic on the evaluation of today's biotechnology technology. The diffusion of the technology is controlled by four factors: machine intelligence, security intelligence, collaborative intelligence and collective intelligence [Figure 5.5]. The machine intelligence considers a set of important criteria such as dominant design features, construction materials, system performance, biocompatibility and ease of use and deployment. It is essential to understand the fundamental principles, functions and mechanisms of the aforesaid biological organs through innovative experimental set up. The security intelligence considers safety, reliability, consistency, efficient surgical operation and reduced risk of infection. The design of biomedical devices must consider biological, chemical, mechanical, electrical and human factors of safety rationally. The collaborative intelligence demands proper integration and coordination among patient care chain, design chain and supply chain of biomedical engineering. The collective intelligence is determined by efficient demand, supply and capacity management of critical resources. Another critical success factor of technology diffusion is correctness and rationality of scope analytics. For example, oral insulin has more strength and opportunities of growth as compared to artificial pancreas. The technology of artificial kidney and liver should explore the hidden potential of tissue engineering. On the other side, the technology of artificial cardiovascular devices and limbs should explore the strength of mechanical and electrical engineering and mechatronics. It is also an interesting research agenda to explore the scope of living biological organ transplantation through organ donation, organ banks and alternative medicines (e.g. integrated medicine, regenerative medicine, precision medicine) as a part of proactive and reactive healthcare approaches. Finally, deep analytics can streamline the diffusion of biomedical technology through efficient coordination and integration among 7-S elements.

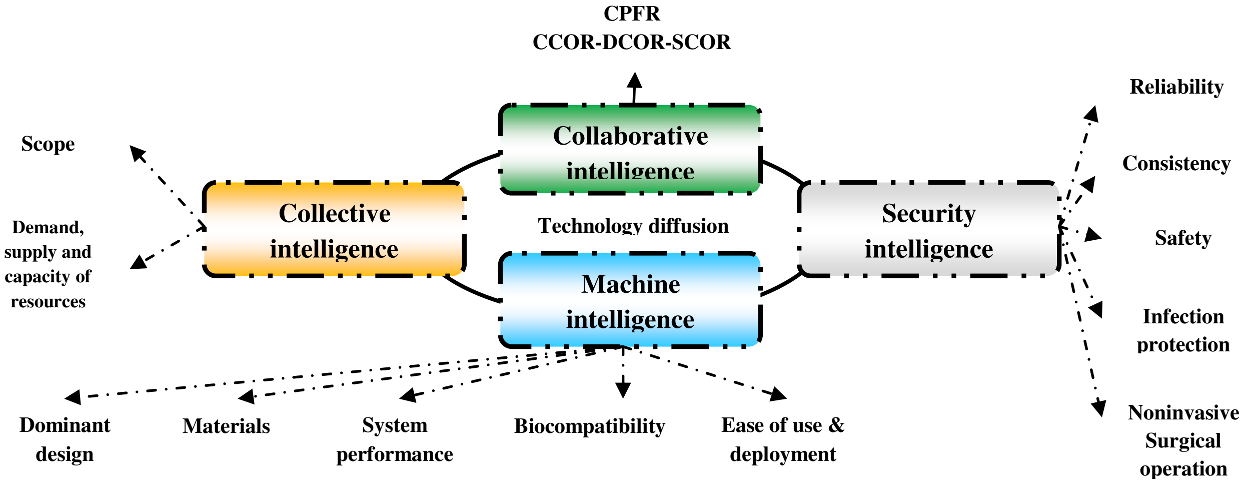


Figure 5.5: Technology diffusion of biomedical technology

This session presents artificial immune system mechanism (AIM). It is a new approach of epidemic and pandemic outbreak control. The basic building block of the mechanism is an analytics having multidimensional view of intelligent reasoning. The mechanism evaluates innate and adaptive system immunity in terms of collective, machine, security, collaborative and business intelligence. It is possible to redefine an efficient global healthcare policy for improved immunity and sustainable physical, mental and social health through reduction of artificial physical and mental stress. A biological system ensures optimal level of immunity by balancing natural and artificial intelligence (AI) based on intelligent reasoning. Effective control of epidemic and pandemic outbreak demands the innovation of smart biomedical devices such as non-contact infrared forehead thermometer. The digital thermal scanner is expected to have a set of important features such as capability to measure body temperature range with accuracy (e.g.0.3^0 C), ^{0}C / ^{0}F options, LCD backlight display, high or low body temperature indicator, high temperature alarm, auto power off after 15 seconds and warranty of one year.

The contribution of the present work is as follows. This novel concept of artificial immune mechanism has been applied to resolve the conflict between security intelligence and business intelligence for mitigating the risk of bio-terrorism today. The review of existing literature could not find out efficient mechanisms to counter bio-terrorism from the perspectives of security intelligence and business intelligence. The security intelligence has been defined weakly, incompletely and imprecisely. The system lacks intelligent model checking or system verification mechanisms based on rational threat analytics. The research methodology adopted in the present work includes case based reasoning, threat analytics and review of relevant literature on cryptography, secure multi-party computation and bio-terrorism. The logic of the bio-terrorism mechanism is explored through hypothetical case based reasoning on healthcare service chain, life-science supply chain, bio-technology and medical practice. The security intelligence is explored through threats analytics on malicious business intelligence.

A human agent must have common sense healthcare knowledge base for proper biological system control through intelligent self-assessment, self-confidence, life-style, diet control and right decision making at right time. It demands the necessity of learning the basic concept of AI reasoning, immunology and common sense healthcare from the childhood through an effective education and knowledge management system. It is not bio-inspired AI but the envision of AI inspired biological system which has a great potential to resolve the global healthcare problems significantly. AI has imagined the product concepts of highly complicated and costly artificial human organs such as artificial brain, heart, lungs, kidney, liver, pancreas, intestine, limbs, neural system, blood and cells though there are technological limitations and financial constraints of biomedical electronics, instrumentation, mechatronics, robotics, computational intelligence and materials science and also critical immunity issues. It is hard to develop and simulate artificial organs due to the inherent complexities of structure, material and mechanisms of the biological system. There are various risks of adaptive immunity and transmission of deadly diseases in artificial organ transplantation, artificial reproduction, common immunization programmes and breast milk feeding to the infants. Relaxation music, yoga and meditation is expected to be a good solution for the treatment of mental health though the modern entertainment world is getting flooded with 'boom boom digital dhamaka' and panic buttons through digital media and horror movies. AIM may be able to overcome some of those practically feasible constraints of the aforesaid imaginative reasoning through intelligent analytics and reasoning. AI community needs a new broad outlook, imagination and dreams to solve a complex problem through a set of simple mechanisms and solutions. Life is beautiful, let us apply AI for rational social choice to save the world.

FURTHER READING

- **B. W. Stewart, C. P. Wild, Eds., World Cancer Report 2014, IARC, France.**
- **C.Tomasetti and B.Vogelstein. 2015. Cancer etiology. Variation in cancer risk among tissues can be explained by the number of stem cell divisions. *Science,* 347(6217):78–81.**
- **A.Albini, F. Tosetti and VW Li. 2012. Cancer prevention by targeting angiogenesis. *Nat Rev Clin Oncol*. 9(9):498–509.**
- **G. Anthes. 2013. Deep learning comes of age. *Communications of the Association for Computing Machinery (ACM)*, 56(6):13–15.**
- **I. Arel, C. Rose, and T. Karnowski. 2010. Deep machine learning — a new frontier in artificial intelligence. *IEEE Computational Intelligence Magazine*,5:13–18.**
- **Y. Bengio. 2013. Deep learning of representations: Looking forward. In *Statistical Language and Speech Processing*, pages 1–37. Springer.**
- **L. Deng. 2011. An overview of deep-structured learning for information processing. In *Proceedings of Asian-Pacific Signal & Information Processing Annual Summit and Conference (APSIPA-ASC)*. October 2011.**
- **N. Nisan and A.Ronen. 1999. Algorithmic mechanism design. In 31st Annual ACM symposium on Theory of Computing, pp 129 -140.**

- **S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Indian Institute of Management Calcutta, India.**
- **A.Barth, B.Rubinstein, M.Sundararajan, J.Mitchell, D.Song and P.L. Bartlett. 2010. A learning-based approach to reactive security. In: Radu, S. (ed.) Financial Cryptography' 2010. LNCS, vol. 6052, pp. 192–206. Springer.**
- **R.Bohme and T.W.Moore. 2009. The iterated weakest link: A model of adaptive security investment. In: Workshop on the Economics of Information Security (WEIS), University College, London, UK.**
- **Y. Lindell. 2003. Composition of secure multi-party protocols a comprehensive study. Springer.**
- **R.Canetti, U.Feige, O.Goldreich and M.Naor. 1996. Adaptively secure multi-party computation.**
- **M.Kearns and M. Li. 1993. Learning in the presence of malicious errors. SIAM Journal on Computing 22(4), 807–837.**
- **M.Barreno, B.Nelson, R. Sears, A.D. Joseph and J.D.Tygar. 2006. Can machine learning be secure? In Proceedings of the ACM symposium on Information, computer, and communications security.**
- **S.Chakraborty. 2015. Secure multi-party computation: how to solve the conflict between security and business intelligence. Technical report.**
- **S.K.Chaturvedi. 2012. Psychiatric oncology: cancer in mind. Indian Journal Psychiatry. Apr-Jun; 54(2): 111–118.**
- **T.V.Borght, S. Asenbaum, P.Bartenstein, C.Halldin, Ö. Kapucu, K.V. Laere, A. Varrone and K.Tatsch. 2010. Brain Tumor Imaging: European Association of Nuclear Medicine Procedure Guidelines.**
- **M. Havaeia, A. Davyb, D. Warde-Farley, A. Biard, A. Courvillec, Y. Bengioc, C. Pal, P.Jodoina and H. Larochelle. 2016. Brain Tumor Segmentation with Deep Neural Networks.**
- **R.L.Siegel, K.D.Miller and A. Jemal. 2015. Cancer statistics. CA Cancer J Clin. 65(1):5–29.**
- **American Cancer Society. 2015. Breast Cancer Facts and Figures 2015–2016: Atlanta: American Cancer Society, Inc.**
- **D. Wang, A. Khosla, R. Gargeya, H.Irshad and A.B. Beck. 2016. Deep Learning for Identifying Metastatic Breast Cancer.**
- **American Cancer Society. 2014.*American Cancer Society: Cancer Facts and Figures 2014*. Altanta, GA: American Cancer Society..**
- **R.Siegel, D.Naishadham and A. Jemal. Cancer statistics, 2012. *CA Cancer J Clin*. 62(1):10-29.**
- **S.Deuffic, et al. 1998. Trends in primary liver cancer. *Lancet.* 1998;351(9097):214-215.**
- **R.Govindan, N. Page and D. Morgensztern. 2006. Changing epidemiology of small-cell lung cancer in the United States over the last 30 years: analysis of the surveillance, epidemiologic, and end results database. *J Clin Oncol*. 24(28):4539-4544. PMID: 17008692.**

- **LC Caprario, DM Kent and GM Strauss. 2013. Effects of chemotherapyon survival of elderly patients with small-cell lung cancer: analysis of the SEER-medicare database. *J Thorac Oncol*. 8(10):1272-1281. PMID: 24457238. PMCID: 3901951.**
- **F.Barbone, M. Bovenzi, F Cavallieri and G. Stanta. 1997. Cigarette smoking and histologic type of lung cancer in men. Chest. 112(6):1474-1479. PMID: 9404741.**
- **S. Faderl S, S. O'Brien S and C-H Pui 2010. Adult acute lymphoblastic leukemia: concepts and strategies. *Cancer*. 116(5):1165-1176.**
- **T.J. Lightfoot and E. Roman. 2004. Causes of childhood leukemia and lymphoma. *Toxicol Appl Pharmacol*. 199(2):104-117.**
- **M. Murai and M. Oya. 2004. Renal cell carcinoma: etiology, incidence and epidemiology. Curr Opin Urol ;14: 229–33.**
- **JD Mulder, HE Schütte, HM Kroon and W.K., Taconis. Radiologic atlas of bone tumors. 2nd edn. Amsterdam: Elsevier; 1993.**
- **A.G. Huvos 1991. Bone tumors. Diagnosis, treatment, and prognosis. 2nd edn. Philadelphia: W.B. Saunders Company.**
- **J.Ferlay, I.I.Soerjomataram and R. Dikshit 2015. Cancer incidence and mortality worldwide: sources, methods and major patterns in GLOBOCAN. *Int J Cancer*. 2015;136:E359–E386.doi:10.1002/ijc.29210.**
- **BK Edwards, A-M Noone, AB Mariotto et al. 2014. Annual Report to the Nation on the status of cancer, 1975-2010, featuring prevalence of comorbidity and impact on survival among persons with lung, colorectal, breast, or prostate cancer. *Cancer*.120(9):1290–1314.**
- **D. Hanahan , R.A. Weinberg, Hallmarks of cancer: the next generation, Cell 144 (5) (2011) 646–674 .**
- **K. Kourou , T.P. Exarchos , K.P. Exarchos , M.V. Karamouzis , D.I. Fotiadis , Ma- chine learning applications in cancer prognosis and prediction, Comput. Struct. Biotechnol. J. 13 (2015) 8–17 .**
- **E. Sayed , A. Wahed , I.A . Emam , A . Badr, Feature selection for cancer classifica- tion: an SVM based approach, Int. J. Comput. Appl. 46 (8) (2012) 20–26.**
- **A. Statnikov , L. Wang , C.F. Aliferis , A comprehensive comparison of random forests and support vector machines for microarray-based cancer classification., BMC Bioinform. 9 (1) (2008) 1–10 .**
- **S.B. Cho , H.H. Won , Machine learning in DNA microarray analysis for cancer classification, in: Asia-Pacific Bioinformatics Conference, 2003, pp. 189–198 .**
- **H. Hijazi , C. Chan , A classification framework applied to cancer gene expression profiles, J. Healthc. Eng. 4 (4) (2012) 255–284.**
- **N. C. F. Codella, Q. B. Nguyen, S. Pankanti, D. A. Gutman, B. Helba, A. C. Halpern, J. R. Smith, Deep learning ensembles for melanoma recognition in dermoscopy images, IBM Journal of Research and Development 61 (4) (2017) 5:1 – 5:15.**

- G. Karakoulas, J. Shawe-Taylor, Optimizing classifiers for imbalanced training sets, in: The Conference on Advances in Neural Information Processing Systems II, MIT Press, Cambridge, MA, USA, 1999, pp. 253– 259.
- [42] R. Rasti, M. Teshnehlab, S. L. Phung, Breast cancer diagnosis in dce-mri using mixture ensemble of convolutional neural networks, Pattern Recognition 72 (2017) 381–390.
- Nussinov, R. Advancements and Challenges in Computational Biology. PLoS Comput. Biol. 2015, 11 (1).
- LeCun, Y.; Bengio, Y.; Hinton, G. Deep Learning. Nature 2015, 521 (7553), 436−444.
- Schmidhuber, J. Deep Learning in Neural Networks: An Overview. Neural Networks 2015, 61, 85−117.
- Fakoor, R.; Huber, M. Using Deep Learning to Enhance Cancer Diagnosis and Classification. In Proceeding 30th Int. Conf. Mach. Learn. Atlanta, GA, 2013, Vol. 28.
- https://www.cancer.gov/about-cancer/treatment/types/surgery/lasers-fact-sheet
- Lu YF, Goldstein DB, Angrist M, Cavalleri G (July 2014). "Personalized medicine and human genetic diversity". Cold Spring Harbor Perspectives in Medicine. 4 (9): a008581. doi:10.1101/cshperspect.a008581. PMC 4143101. PMID 25059740.
- "N-of-One: Tailored Clinical Molecular Test Interpretation". n-of-one.com.
- Blau CA, Liakopoulou E (January 2013). "Can we deconstruct cancer, one patient at a time?". Trends in Genetics. 29 (1): 6–10. doi:10.1016/j.tig.2012.09.004. PMC 4221262. PMID 23102584.
- Garraway LA, Verweij J, Ballman KV (May 2013). "Precision oncology: an overview". Journal of Clinical Oncology. 31 (15): 1803–5. doi:10.1200/jco.2013.49.4799. PMID 23589545.
- Shrager J, Tenenbaum JM (February 2014). "Rapid learning for precision oncology". Nature Reviews. Clinical Oncology. 11 (2): 109–18. doi:10.1038/nrclinonc.2013.244. PMID 24445514.
- Ashley EA (June 2015). "The precision medicine initiative: a new national effort". JAMA. 313 (21): 2119–20. doi:10.1001/jama.2015.3595. PMID 25928209.
- Ashley EA (August 2016). "Towards precision medicine". Nature Reviews. Genetics. 17 (9): 507–22. doi:10.1038/nrg.2016.86. PMID 27528417.
- Mesko B (2017). "Expert Review of Precision Medicine and Drug Development". Journal Expert Review of Precision Medicine and Drug Development. 2 (5): 239–241. doi:10.1080/23808993.2017.1380516.
- Ray A. "Artificial Intelligence and Blockchain for Precision Medicine". Inner Light Publishers. Retrieved 21 May 2018.
- Krittanawong C, Zhang H, Wang Z, Aydar M, Kitai T (May 2017). "Artificial Intelligence in Precision Cardiovascular Medicine". Journal of the American College of Cardiology. 69(21): 2657–2664. doi:10.1016/j.jacc.2017.03.571. PMID 28545640.

- **Mason, Chris; Dunnill, Peter (2008). "A brief definition of regenerative medicine". Regenerative Medicine. 3 (1): 1–5. doi:10.2217/17460751.3.1.1. ISSN 1746-0751. PMID 18154457.**
- **Mahla RS (2016). "Stem cells application in regenerative medicine and disease threpeutics". International Journal of Cell Biology. 2016 (7): 1–24. doi:10.1155/2016/6940283. PMC 4969512. PMID 27516776.**
- **Mason C; Dunnill P (January 2008). "A brief definition of regenerative medicine". Regenerative Medicine. 3 (1): 1–5. doi:10.2217/17460751.3.1.1. PMID 18154457.**
- **Regenerative medicine glossary". Regenerative Medicine. 4 (4Suppl): S1–88. July 2009. doi:10.2217/rme.09.s1. PMID 19604041.**
- **Riazi AM; Kwon SY; Stanford WL (2009). Stem cell sources for regenerative medicine. Methods in Molecular Biology. 482. pp. 55–90. doi:10.1007/978-1-59745-060-7_5. ISBN 978-1-58829-797-6. PMID 19089350.**
- **Lysaght MJ; Crager J (July 2009). "Origins". Tissue Engineering. Part A. 15 (7): 1449–50. doi:10.1089/ten.tea.2007.0412. PMID 19327019.**
- **https://www.nsf.gov/pubs/2004/nsf0450/ Viola, J., Lal, B., and Grad, O. The Emergence of Tissue Engineering as a Research Field. Arlington, VA: National Science Foundation, 2003.**
- **Haseltine, WA (6 July 2004). "The Emergence of Regenerative Medicine: A New Field and a New Society". E-biomed: The Journal of Regenerative Medicine. 2 (4): 17–23. doi:10.1089/152489001753309652.**
- **Mao AS, Mooney DJ (Nov 2015). "Regenerative medicine: Current therapies and future directions". Proc Natl Acad Sci U S A. 112 (47): 14452–9. doi:10.1073/pnas.1508520112. PMC 4664309. PMID 26598661.**
- **A. Nautiyal, N.V.M. Satheesh and S. Bhattacharya. 2013. A detailed review on diabetes mellitus and its treatment in allopathic and alternative systems. Int J Adv Pharm Sci ;4:16-43.**
- **H. Iyer, A. Khedkar and M. Verm. 2010. Oral insulin – a review of current status. Diabetes, Obesity and Metabolism. 12: 179–185.**
- **C. Reis, R. Neufeld, A. Ribeiro A and F. Veiga . 2006. Nanoencapsulation I. Methods for preparation of drug-loaded polymeric nanoparticles. Nanomedicine; 2: 8-21.**
- **M.S. Bhadoria and P. Mishra. 2013. Applications of nanotechnology in diabetes. Int. J. Res. Comput. Eng. Electron., 2.**
- **P. Home. Insulin therapy and cancer. Diabet. Care, 2013, 36(Suppl2), S240-244.**
- **S.Kalra. 2013. Advances in insulin therapy. J. Pak. Med. Assoc., 63, 925-927.**
- **S. Kalra, B.Kalra and N. Agrawal. 2010. Oral insulin. Diabetol. Metab.Syndr., 2, 66.**
- **P.Mukhopadhyay, R.Mishra, D.Rana and P.P. Kundu. 2012. Strategies for effective oral insulin delivery with modified chitosan nanoparticles: A review. Prog. Polym. Sci., 37, 1457-1475.**

- **S.R.Joshi, R.M.Parikh and A.K. Das. Insulin - History, biochemistry, physiology and pharmacology. J Assoc Physicians India 2007;55 Suppl:19-25.**
- **A. Akbarzadeh, R. Rezaei-Sadabady, S.Davaran, S.W. Joo, N. Zarghami and Y. Hanifehpour. Liposome: Classification, preparation, and applications. Nanoscale Res Lett 2013;8:1-9.**
- **X. Zhang, J. Qi , Y.Lu , W.He, X. Li and W. Wu 2014. Biotinylated liposomes as potential carriers for the oral delivery of insulin. Nanomedicine 2014;10:167-76.**
- **E. Zijlstra, L. Heinemann and L. Plum-Mörschel. Oral insulin reloaded: A structured approach. J Diabetes Sci Technol 2014;8:458-65.**
- **X.Xiongliang, Z. Hongyu, Z., L. Long and C. Zhipeng. 2012. Insulin nanoparticle and preparation method thereof. Chinese Patent 1,026,144,98, August.**
- **L. Huixia, S.LA, Z. Zhenhai and Z. Jianping. 2011. Preparation and application of novel oral insulin nanoparticles. Chinese Patent 1,021,207,81, July 13, 2011.**
- **P. Wang, Y. Cheng, Y. and D. Du. 2003. Nano-insulin oral preparation. Chinese Patent 2,566,851, August. .**
- **Z. Zhang, Z. Hou, Z and J. Niu. 2003. Process for preparing oral insulin nanomaterial. Chinese Patent 1,425,464, June .**
- **R.Margalit. 2003. Liposome-encapsulated insulin formulations. Australian Patent 2,002,330,273, April.**
- **P.D.Light. 2004. Dialysate composition in hemodialysis and peritonial dialysis, in Henrich WL (ed.), Principles and Practice of Dialysis. pp. 28–44.**
- **W. Henrich. 2004. Prinicples and Practice of Dialysis, Philadelphia, Pa. Lippincott Williams & Wilkins.**
- **.Ronco and N.W. Levin. 2004. Hemodialysis, Vascular Access, and Peritoneal Dialysis Access. New York.**
- **N.A.Hakim. 1998. Influence of hemodialysis membrane on outcome of ESRD patients. Am. J. Kidney Dis.32:71–75.**
- **M. Misra. 2005. The basics of hemodialysis equipment. Hemodial. Int. 9:30–36,.**
- **A. O'Connor and B. Wish. 2004. Hemodialysis adequacy and timing of dialysis initiation, in Henrich WL (ed.), Principles and Practice of Dialysis. Philadelphia, pp. 111–127.**
- **V.A. Kumar and T.A. Depner. 2004. Approach to hemodialysis kinetic modeling, in enrich WL (ed.), Principles and Practice of Dialysis, Philadelphia, Pa. Lippincott Williams & Wilkins, 3d ed., 2004, pp. 82–102.**
- **J.K. Leypoldt. 1999. The Artificial Kidney: Physiological Modeling and Tissue Engineering, Austin, Tex, R.G. Landes.**
- **O.F. Bertrand and R. Sipehia. 1998. Biocompatibility aspects of new stent technology. J Am Coll, Cardiol, 32(3):562–71.**
- **M. Kutz (Ed.). 2009. Handbook of Biomedical Engineering and Design. McGraw-Hill**

- **N. L’Heureux and N. Dusserre,. 2007. Technology insight: the evolution of tissue-engineered vascular grafts - from research to clinical practice. Nat Clin Pract Cardiovasc Med, 4(7):389–95.**
- **A. J. Makarewicz and L. F. Mockros. 1994. A pumping artificial lung. ASAIO J, 40(3):M518–21.**
- **M.A. Mattos and K. J. Hodgson. 1999. Vascular stents. Curr Probl Surg, 36(12):909–1053.**
- **A.W. Holt. 1999. Acute liver failure. Crit Care Resusc. 1:25–38. [PubMed]**
- **JG Freeman , K.Matthewson and C.O. Record. 1986. Plasmapheresis in acute liver failure. Int J Artif Organs. 9:433–438. [PubMed]**
- **L.J. Li, Y.M. Zhang, X.L. Liu, W.B.Du, J.R. Huang, Q.Yang, X.W. Xu XW and Y.M. Chen . 2006. Artificial liver support system in China: A review over the last 30 years. Ther Apher Dial.10:160–167.**
- **C.D.Campli, R. Gaspari, V. Mignani, G.Stifano, A. Santoliquido , L.Z. Verme, R. Proietti, P. Pola, N.G. Silveri, G.Gasbarrini and A. Gasbarrini. 2003. Successful MARS reatment in severe cholestatic patients with acute on chronic liver failure. Artif Organs. 27:565–569.**
- **C.Doria, L.Mandala, V.L. Scott, S.Gruttadauria, I.R. Marino. 2006. Fulminant hepatic failure bridged to liver transplantation with a molecular adsorbent recirculating system: A single-center experience. Dig Dis Sci.;51:47–53.**
- **M.P. van de Kerkhove, E. Di Florio, V. Scuderi, A. Mancini, A. Belli, A. Bracco, D. Scala, S. Scala, L. Zeuli, G. Di Nicuolo, P. Amoroso, F.Calise, R.A. Chamuleau. 2003. Bridging a patient with acute liver failure to liver transplantation by the AMC-bioartificial liver. Cell Transplant.12:563–568.**
- **T.K. Ulrich and S.D. Eppinger. 2000. Product Design and Development, 2nd ed., McGraw-Hill.**
- **S.C. Wheelwright and K.B. Clark. 1992. Revolutionizing Product Development. Free Press.**
- **A.L. Swiffin et al. 1987. Adaptive and predictive techniques in a communication prosthesis, *Augmentative and Alternative Communication,* 3(4):181–191.**
- **J. Kumagai . 2004. Talk to the machine, *IEEE Spectrum,* 39(9):60–64, 2004.**
- **R.W. Beasley and G.M. de Bese. 1990. *Prosthesis for the Hand. Surgery of the Musculoskeletal System*, 2nd ed. New York**
- **C.D. Brenner. 2004. Wrist Disarticulation and Transradial Amputation: Prosthetic Management. In: *Atlas of Amputations and Limb Deficiencies*, 3rd ed. (Smith DG, Michael JW, Bowker JH, eds.), pp. 223–230.Rosemont, Ill.: American Academy of Orthopaedic Surgeons.**
- **D. Childress. 1985. Historical aspects of powered limb prosthetics. *Clinical Prosthetics and Orthotics* 9:2–13.**
- **W. Daly. 2004. Elbow Disarticulation and Transhumeral Amputation: Prosthetic Management. In: *Atlas of Amputations and Limb Deficiencies*, 3rd ed. (Smith DG, Michael JW, Bowker JH, eds.), pp. 234–249.Rosemont, Ill.: American Academy of Orthopaedic Surgeons.**

- **M.J. Fletcher. 1954. New Developments in Hands and Hook. In: *Human Limbs and Their Substitutes* (Klopsteg PE, Wilson PD, eds.), pp. 359–408.McGraw-Hill.**
- **Kenworthy G. 1974. An artificial hand incorporating function and cosmesis. *Bio-Medical Engineering,* 9:559–562.**
- **Y. Lozac'h, S. Madon, S. Hubbard and G. Bush. 1992. On the Evaluation of a Multifunctional Prosthesis. In:*Proceedings of the 7th World Congress of the International Society for Prosthetics and Orthotics (ISPO)*, p. 185.Chicago, Ill.**
- **J.W. Michael. 1986. Upper-limb powered components and controls: current concepts. *Clinical Prosthetics and Orthotics* 10:66–77.**
- **D.G. Smith, J.W. Michael JW and J.H. Bowker. 2004. *Atlas of Amputations and Limb Decifiencies*, 3rd ed. Rosemont, Ill.: American Academy of Orthopaedic Surgeons.**
- **C.L.Taylor.1954. The Biomechanics of the Normal and of the Amputated Upper Extremity. In: *Human Limbs and Their Substitutes* (Klopsteg PE, Wilson PD, eds.), McGraw-Hill, New York.**
- **D. G. Shurr and T. M. Cook. 1990. *Prosthetics and Orthotics,* Appleton & Lange, East Norwalk, Conn.**
- **A. B. Wilson. 1989. *Limb Prosthetics,* 6th ed., Demos Publications, New York, N.Y.**
- **B. J. May. 1996. *Amputations and Prosthetics: A Case Study Approach,* F. A. Davis, Philadelphia, Pa.**
- **W. Loob. 2001. Robotics and electronics research aid building "smart" prostheses, *in Medical Device and Diagnostic Industry,* Jan., 64.**
- **K.S. Katti 2004. Biomaterials in total joint replacement. *Colloids Surf B Biointerfaces*, 39:133–142.**
- **I.C.Clarke, T.Donaldson, J.G.Bowsher, S.Nasser and T.Takahashi. 2005. Current concepts of metal-onmetal hip resurfacing. *Orthop Clin N Am*, 36:143–162.**
- **M.P. Gispert, A.P. Serro, R.Colaco, E. Pires and B. Saramago. 2007. Wear of ceramic coated metal-on-metal bearings used for hip replacement. *Wear*, 263:1060–1065.**
- **I.D. Learmonth, C.Young and C. Rorabeck. 2007. The operation of the century: total hip replacement. *Lancet*, 370:1508–1519.**
- **Abiomed Inc. 2007. Heart Replacement.**
- **J. Al Suwaidi, P. B. Berger et al.. 2000. Coronary artery stents. *JAMA*, 284(14):1828–36.**
- **J. Bai and H. Lin et al. 1994. A study of optimal configuration and control of a multi-chamber balloon for intraaortic balloon pumping. *Ann Biomed Eng*, 22(5):524–31.**
- **O.F.Bertrand, R. Sipehia et al. 1998. Biocompatibility aspects of new stent technology. *J Am Coll*, *Cardiol*, 32(3):562–71.**
- **https://www.cancer.gov/about-cancer/treatment/types/surgery/lasers-fact-sheet**
- **http://lasermart.in/lasotronix-smart-pro-dental.html**

- **N.Bostrum. 2014. Super intelligence: Path, dangers, strategies. Oxford University Press.**
- **D. Perlis. 2016. Five dimensions of reasoning in the wild. AAAI.**
- **D. Dasgupta (ed). 1999. Artificial Immune Systems and Their Applications. Springer.**
- **D.Dasgupta and F.Gonzalez. 2002. An immunity-based technique to characterize intrusions in computer networks. IEEE Trans Evol Comput 6:1081–1088.**
- **J.D.Farmer, N.H. Packard and A.S. Perelson. 1986. The immune system, adaptation, and machine learning. Physica 22:187–204.**
- **E.Hart and J.Timmis. 2008. Application areas of AIS: the past, the present and the future. Appl Soft Comput 8:191–201.**
- **S.Forrest, A.S. Perelson, L. Allen and R. Cherukuri. 1994. Self–nonself discrimination in a computer. In: Proceedings of the IEEE symposium on research in security and privacy, Oakland, CA, USA, pp 202–212.**
- **S. Hofmeyr and S. Forrest. 2000. Architecture for an artificial immune system. Evol Comput 7:1289–1296.**
- **E.Rich and K. Knight. 1991. Artificial intelligence, 2nd edn. McGraw-Hill, New York.**
- **G.Luger. 2005. Artificial intelligence: structures and strategies for complex problem solving, 5th edn. Addison-Wesley, New York.**
- **A.Cawsey. 1998. The essence of artificial intelligence. Prentice-Hall, Englewood Cliffs.**
- **P. Norvig. 1992. Paradigms of Artificial Intelligence Programming: Case Studies in Common Lisp. Morgan Kaufmann.**
- **S. J. Russell and E. H. Wefalld. 1991. Do the Right Thing: Studies in Limited Rationality. MIT Press.**
- **A. Konar. 1999. Artificial Intelligence and Soft Computing. CRC Press.**
- **J.Kim, P.Bentley, U.Aickelin, J.Greensmith, G.Tedesco and J.Twycross J. 2007. Immune system approaches to intrusion detection - a review. Nat Comput 6:413–466.**
- **P.Matzinger. 1994. Tolerance, danger and the extended family. Ann Rev Immunol12:991–1045.**
- **P.Matzinger. 2001. The danger model in its historical context. Scand J Immunol 54:4–9.**
- **P.Matzinger. 2002. The danger model: a renewed sense of self. Science 296:301–305.**
- **L. Castro and C.J.Timmis. 2002. Artificial Immune Systems : A New Computational Intelligence Approach. Springer.**
- **A.O.Tarakanov, V.A.Skormin and S.P.Sokolova. 2003. Immunocomputing: Principles and applications. Springer.**
- **J.Douceur. 2002. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS).**
- **A.K.Pal, D. Nath and S.Chakraborty. 2010. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor. WASET, Brazil.**

- **S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Indian Institute of Management Calcutta, India.**
- **G.Kol and M.Naor. Cryptography and game theory: Designing protocols for exchanging Information. Proceedings from 5th Theory of Cryptography Conference (TCC), 2008.**
- **W. Du. A study of several specific secure two-party computation problems. Doctoral dissertation, Purdue University, USA. 2001.**
- **Y. Lindell. Composition of secure multi-party protocols a comprehensive study. Springer. 2003.**
- **S.Chakraborty. A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Doctoral dissertation (unpublished), Indian Institute of Management Calcutta, 2007.**
- **A.L.Melnick. Biological, chemical and radiological terrorism. Springer, NY,USA, 2008.**
- **S. Chakraborty. Security intelligence for broadcasts: Threat analytics. Technical report. 2012.**
- **J.Douceur. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS). 2002.**
- **A.K.Pal, D. Nath and Chakraborty, S. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor, WASET, Brazil.2010.**
- **M.Shema. edited by A.Ely. Seven deadliest web application attacks. Elsevier. 2010.**
- **F.A.Kuglin. Pharmaceutical supply chain drug quality and security act. CRC Press, Taylor & Francis Group, Boca Raton, USA.**
- **G.Ateniese, R.Curtmola, B. Medeiros and D.Davis. Medical information privacy assurance: Cryptographic and system aspects, Technical Report, John Hopkins University. 2003.**
- **M.Gertz and S.Jajodia. Handbook of database security applications and trends. 2008.**
- **B. Schneier. Applied Cryptography, John Wiley, New York,1996.**
- **W.Mao. Modern Cryptography Theory & Practice, Pearson Education. 2007.**
- **Y.Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). LNCS 1318, Springer-Verlag.**

Quiz

- **Explain the technology of deep learning on prediction and prevention for cancer care? Justify it as a technology for humanity. What is the scope of this technology?**
- **What is the dominant design of the technology?**
- **What are the basic elements of the system architecture?**

- **What do you mean by technology security in cancer care? How to verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion for cancer care? What is the outcome of technology life-cycle analysis?**
- **How to manage resources for this innovation project?**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How to manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
- **Develop a deep learning algorithm for the prediction of cancer correctly?**
- **Explain the scope of regenerative, integrated, alternative, genomics and precision medicine for cancer care through SWOT analysis.**
- **Explain the technology of biomedical instrumentation for cancer care? Justify it as a technology for humanity. What is the scope of biomedical instrumentation technology?**
- **What is the dominant design of the biomedical technology?**
- **What are the basic elements of the system architecture?**
- **What do you mean by technology security in biomedical instrumentation? How to verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion of biomedical instrumentation for cancer care? What is the outcome of technology life-cycle analysis?**
- **How to manage resources for this innovation project?**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How can You manage technology innovation project efficiently for biomedical instrumentation? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
- **Explain the scope of laser therapy, pervasive computing and surgical robotics for cancer care from the test cases stated in section 9.**
- **Can you design an automated biomedical test kit for cancer care? Show the system architecture.**
- **What is artifial immune system? How can it control epidemic and pandemic outbreak?**
- **What are the basic elements of system architecture for disaster control? How to represent the structure correctly?**
- **What do you mean by technology security for artificial immune system? How to verify the security intelligence? What is bioterrorism? How to assess and mitigate risks of bioterrorism globally?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis?**

- **How to manage resources for disaster management? What should be the talent management strategy?**
- **What are the skills, leadership style and support demanded by the technological innovation?**
- **How to manage technology innovation project efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements for disaster management?**

APPENDIX

This section highlights the application of DACPM for nine different types of cancer.

A. Cancer of Mind

Psycho-oncology : Psychiatric oncology is the study of psychiatric and social aspects of cancer such as cause, maintenance and prognosis of cancer, emotional reactions, psychiatric disorders, stress management and communication skills of the oncologists in revealing bad news and handling difficult questions and counseling. It is essential to understand psycho-neuro-endocrino-immunological mechanisms of the cancer patients. The psychological responses to cancer arise from knowledge of life-threatening diagnosis, uncertainty, financial burden and fear of death. The emotional responses arise from pain, nausea and unwanted side-effects of medical, surgical, and radiation treatments. This treatment also addresses various issues such as diet and nutritional supplements, yoga, meditation and physical exercises and aromatherapy.

B. Neural control and coordination

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human nervous system, sensory system;
Objectives: cancer prevention at optimal cost; focus : brain cancer [18,19];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- ♦ **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
  - **Identify targets**
    - **application schema : Nervous and sensory system;**
    - **networking schema :**
      - **Nervous system : CNS – Brain, spinal chord; PNS, Neurons, nerves, cerebrospinal fluid, brain stem, meninges, neuroglia, ependymal cells, neurosecretory cells;, cerebral nerve, spinal nerve;**
      - **Sensory organs : eye, ear, nose, toungue, skin;**
    - **computing schema : nerve impulse, reflex, neurotransmitter, neurosecretion, chemoreception; control and coordination, integration, memory, mechanism of sensory organs – see, hear, smell, feel, taste;**
    - **data schema : sensory receptors – photo, chemo, thermo, electro and mechanoreceptors; structure of sensory organs;**
    - **security schema : immunity, hormones, vitamins, minerals, blood, CSF;**
  - **Threat modeling**
    - **Call threat analytics and assess miscellaneous risk elements**
      - **brain tumors : astrocytic, neuronal, embryonic and pineal;**
      - **disorders of nervous system : memory loss, poliomyelitis, meningitis, sciatica, neuritis, synaptic delay, synaptic fatigue;**
      - **eye defects – myopia, hypermetropia, astigmatism, presbiopia, cataract, glaucoma;**
      - **skin cancer;**
      - **throat cancer;**
    - **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
    - **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
    - **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**
    - **Estimate requirements of healthcare in terms of demand plan (P^p_d);**
    - **Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.**
      - **Optimal diet intake to fight against malnutrition;**
      - **Life-style : yoga and physical activities, stress control through meditation;**
      - **Eye, ear and skin care against hostile climate (e.g. snowfall, scorching sunshine)**
      - **Autoimmunity through vaccination**
- **Reactive approach:**

- **adopt sense-and-respond strategy based on following *symptoms* of brain cancer : headache, weakness, clumsiness, difficulty in walking, seizures, altered mental status like changes in concentration, memory, attention or alertness, intellectual capacity or emotional response, nausea, vomiting, lethargy, blurred vision and difficulty with speech;**
- **assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.**
    - **what is corrupted or compromised : Is the brain tumor malignant or benign?**
    - **time series analysis : what occurred? what is occuring? what will occur?**
    - **insights : how and why did it occur? do cause-effect analysis.**
        - **genetic factors**
        - **environmental effects**
        - **radiation**
        - **HIV infection**
        - **smoking**
    - **recommend : what is the next best action?**
    - **predict: what is the best or worst that can happen?**
- **verify security intelligence of application, computing, networking, security and data schema of biological system.**
    - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**
    - **Level 2: authentication, authorization, correct identification, privacy, audit;**
    - **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**
    - **Level4: stability, system dynamics, quality of application integration.**
- **Explore risk mitigation plan (P^r_d and P^r_m).**
    - **Detection of viable tumor tissue → tumor delineation → selection of the best biopsy site → non-invasive tumor grading → therapy planning →monitoring tumor response;**
    - **MRI and CT scan of brain tumor (Refer Deep Leaning Algorithm of section 5.1);**
    - **Biopsy trough surgery of brain tumor;**
    - **Treating viral and bacterial infection, chronic inflammation, pain;**
    - **Automatic drug injection into malignant brain tumor through nano-chip implanted into brain.**

- **Fight against bad luck : Identify critical risk elements.**
    - **Genetic disorder (sex, race, ethnicity, somatic mutation)**

        - ♦ **Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)**
        - ♦ **Injuries from accidents, war and crime**
        - ♦ **Occupational exposure**
        - ♦ **Environmental pollution (e.g. dust, sound pollution)**
        - ♦ **Hostile climate, weather and other locational disadvantages, exposure to sunshine**
        - ♦ **Malnutrition due to poverty**
    - **Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.**

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

C. Chemical coordination and integration

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human endocrine system;
Objectives: cancer prevention at optimal cost; Focus : breast cancer [20,21];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM);**
- ♦ **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
    - **Identify targets :**

- ♦ **application schema : Endocrine, Exocrine and Heterocrine system, Breast;**
- ♦ **networking schema : Glands – hypothalamus, pituitary, pineal, thyroid, parathyroid, thymus, adrenals, pancreas, gonads : testes and ovaries, kidneys;**
- ♦ **computing schema : coordination between endocrine and nervous system, interaction among glands, hormone action mechanism (formation of Camp);**
- ♦ **data schema : hormones (informational molecules secreted by endocrine cells), hypothalamus – neurohormones > release hormones (RH), inhibitory hormones (IH); pituitary – FSH LH, GTH, TSH, ACTH, GH (*),LTH, OT; pineal – melatonin; thyroid – thyroxine (**), calcitonin; parathyroid – PTH (#), thymus - thymosine, adrenals - aldosterone, glucocorticoids, sexcorticoids (##); pancreas – insulin ($), glucagon, SS; gonads : testes – LH and ovaries – Estrogen, Progesterone and Relaxin; kidneys - Renin; primary, secondary and final targets;**
- ♦ **security schema : innate and adaptive immunity, hormones, vitamins, minerals;**

- **Threat modeling**
  - ♦ **Call threat analytics, understand *molecular switches* and assess miscellaneous risk elements of breast cancer:**
    - ▪ **age (old age increases risk)**
    - ▪ **gender (females with higher risk)**
    - ▪ **race**
    - ▪ **reproductive factors (e.g. infertility, menarche age, menopause age, age of first pregnancy)**
    - ▪ **parity (nulliparous women at higher risk)**
    - ▪ **family history (inherited genetic mutation)**
    - ▪ **obesity and weight**
    - ▪ **breast density (higher density with higher risk)**
    - ▪ **radiation exposure**
    - ▪ **side-effects of hormone replacement therapy, cross-sex hormone therapy and birth controlling pills**
  - ♦ **Assess the risks of other disorders**
    - ▪ **over secretion : gigantism (*); grave's disease(**), osteoporosis (#);**
    - ▪ **deficiency : dwarfism(*), goitre(**), addison's disease (##), diabetes mellitus ($);**
  - ♦ **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
  - ♦ **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
  - ♦ **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**

- ♦ **Estimate requirements of healthcare in terms of demand plan ($P^p{}_d$);**
- ♦ **Explore risk mitigation plan ($P^p{}_m$) : accept / transfer / remove / mitigate risks.**
  - ▪ **Optimal diet intake to fight against malnutrition;**
  - ▪ **Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control through yoga and physical activities, stress control through meditation;**
  - ▪ **Proactive risk mitigation strategies for breast cancer**
    - **Early detection through self-breast examination (SBE) : 'know your breast';**
    - **Rational diet chart, yoga and physical exercises;**
    - **Diabetes control;**
    - **Avoid wearing tight dress;**
    - **Safe massage for beast development exercises;**
    - **Caution: violent love-life**

Reactive approach:

- **adopt sense-and-respond strategy.**
- **assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.**
  - ♦ **what is corrupted or compromised?**
  - ♦ **time series analysis : what occurred? what is occuring? what will occur?**
  - ♦ **insights : how and why did it occur? do cause-effect analysis.**
  - ♦ **recommend : what is the next best action?**
  - ♦ **predict: what is the best or worst that can happen?**
- **verify security intelligence of application, computing, networking, security and data schema of biological system.**
  - ♦ **Level 1: correctness, fairness, accountability, transparency, rationality, commitment;**
  - ♦ **Level 2: authentication, authorization, correct identification, privacy, audit;**
  - ♦ **Level 3: reliability, consistency, liveness, resiliency;**
  - ♦ **Level 4: stability, system dynamics, quality of application integration.**
- **Explore risk mitigation plan ($P^r{}_d$ and $P^r{}_m$).**
  - ♦ **Breast cancer : Personalized screening**
  - ♦ **Do clinical breast examination (CBE) → Data visualization**
    - ▪ **Convolutional network for tumor detection in breast mammography (Refer Deep Leaning Algorithm of section 5.1);**

            - ▪ **Caution of mammography screening : radiation exposure, anxiety, false positives and over diagnosis;**
        - ♦ **Integrated medicine**
        - ♦ **Mastectomies**
- **Fight against bad luck : Identify critical risk elements.**
        - ♦ **Genetic disorder (sex, race, ethnicity, somatic mutation)**
        - ♦ **Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)**
        - ♦ **Side effects of medical treatment (e.g. hormone therapy)**
        - ♦ **Malnutrition due to poverty**
    - **Develop risk mitigation plan in terms of surgical operation, gene therapy, stem cell therapy.**

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

Deep learning algorithm for breast cancer [22] :
Objective: Computer aided breast cancer detection and diagnosis with improved accuracy; avoid the limitations of qualitative visual analysis with microscope like lack of standardization, diagnostic errors and excessive cognitive load, precision medical treatment through computational image analysis;
Input : millions of training patches;
System Architecture: Deep Convolutional Neural Network;
Procedure of cancer metastasis detection :

- **a patch-based classification stage**
- **a heat map based post processing stage**

Output: identification of cancer metastases from whole slide images of breast sentinel lymph nodes; make patch-level predictions to discriminate tumor patches from normal-patches.

D. Digestive system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human digestive system;
Objectives: cancer prevention at optimal cost;

Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of digestive system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
  - **Identify targets**
    - **application schema : digestive system;**
    - **networking schema :**
      - **alimentary canal – mouth, vestibule, oral cavity – tongue, teeth, pharynx, oesophagus, stomach, small intestine, large intestine;**
      - **digestive glands – salivary gland, gastric glands, liver, pancreas, intestinal glands;**
    - **computing schema :**
      - **nutrition mechanisms – autotrophic, holophytic, heterotrophic, symbiotic and holozoic;**
      - **movement of alimentary canal;**
      - **hormonal control of digestive secretion;**
      - **ingestion, digestion - intracellular, extracellular and mixed, egestion, absorption and assimilation;**
    - **data schema : nutrients – food (carbohydrates, protein, fat), minerals, vitamins, bile;**
    - **security schema : immunity, enzymes, bile, gastric juice, hormones, vitamins, minerals;**
  - **Threat modeling**
    - **Call threat analytics and assess miscellaneous risk elements:**
      - **malnutrition, over nutrition,**
      - **incomplete digestive tract,**
      - **Gastrointestinal cancer [23,24,25]**
        - **gastric, gastro esophageal junction and esophageal cancer (adenocarcinoma) with risk elements like low consumption of fruits and vegetables, high intake of N-compounds in salted and preserved foods and occupational exposure in coal mining and nickel, rubber and timber processing industries, high meat consumption,**

smoking, alcohol consumption, gastric surgery and reproductive hormones

- oral cancer
- pancreatic Cancer with risk elements like tobacco smoking, diabetes and chronic pancreatitis, diet, body mass index and genetic syndrome
- hepatocellular carcinoma (HCC) or liver cancer caused by chronic viral hepatitis, alcohol and cirrhosis, aflatoxin, OCP and genetic metabolic factors, toxic exposures of medicine
- small bowel cancer and appendiceal tumors
- colorectal cancer with risk factors such as somatic or inherited genetic mutation, diet, obesity, inflammatory bowel diseases,
- anal cancer
- neuroendocrine tumor

- ♦ Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];
- ♦ Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
- ♦ Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
- ♦ Estimate requirements of healthcare in terms of demand plan (P^p_d);
- ♦ Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
  - Auto-immunity and vaccination against hepatitis B and C;
  - Optimal diet intake to fight against malnutrition;
  - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control through yoga and physical activities
  - Oral cancer from wild polygamy;

Reactive approach:

- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
  - ♦ what is corrupted or compromised?
  - ♦ time series analysis : what occurred? what is occuring? what will occur?
  - ♦ insights : how and why did it occur? do cause-effect analysis.
  - ♦ recommend : what is the next best action?
  - ♦ predict: what is the best or worst that can happen?

- verify security intelligence of application, computing, networking, security and data schema of biological system.
    - ♦ Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;
    - ♦ Level 2: authentication, authorization, correct identification, privacy, audit;
    - ♦ Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;
    - ♦ Level4: stability, system dynamics, quality of application integration.
- Explore risk mitigation plan.
    - ♦ Gastric cancer : surgery, perioperative chemotherapy, postoperative chemoradiotherapy;
    - ♦ Pancreatic cancer : immunotherapy, CT scan, biopsy, surgery, systemic therapy or chemoradiation;
    - ♦ Liver cancer : systemic chemotherapy, hormonal therapy, clinical trial of antiangiogenesis agents, radiation therapy;
    - ♦ Colorectal cancer : fecal occult blood testing, barium x-ray, colonoscopy, sigmoidoscopy, genetic testing, radiotherapy, surgery;
    - ♦ Do medical testing → Data visualization of images (e.g. liver, pancreas and alimentary canal, Refer Deep Leaning Algorithm of section 5.1)
    - ♦ Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
    - ♦ Insulin injection
    - ♦ Artificial liver and pancreas transplantation

Fight against bad luck : Identify critical risk elements.

- ♦ Genetic disorder (sex, race, ethnicity, somatic mutation)
- ♦ Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
- ♦ Injuries from accidents, war and crime
- ♦ Occupational exposure
- ♦ Water and soil pollution
- ♦ Hostile climate, weather and other locational disadvantages, exposure to sunshine
- ♦ Malnutrition due to poverty
- Develop risk mitigation plan in terms of organ transplantation, surgical operation, gene therapy, stem cell therapy and migration of human civilization from risky zone.

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

E. Respiratory system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human respiratory system;
Objectives: cancer prevention at optimal cost; focus : lung cancer [26,27,28];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- ♦ **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
    - **Identify targets**
        - ♦ **application schema : respiratory system;**
        - ♦ **networking schema : respiratory tract, respiratory organs – lungs, tissues, larynx;**
        - ♦ **computing schema : breathing mechanism – inspiration, air filtering, exchange of gases in alveoli, expiration; nervous and chemical control of respiration, transport of gases in blood (O_2, CO_2), artificial respiration mechanism;**
        - ♦ **data schema (^) : respiratory rate, pulmonary air volume and capacity, composition of inspired, expired and alveolar air, TV, IRV,ERV,RV,VC,IC,FRC,TLC;**
        - ♦ **security schema : innate and adaptive immunity, hormones, blood;**
    - **Threat modeling**

- ♦ Call threat analytics function and assess miscellaneous risk elements : lung cancer,
  - ▪ Lung cancer : small cell and non-small cell lung cancer
    - Tobacco exposure: duration and intensity of tobacco use;
    - Exposure to asbestos, benzene, coal tar and radon gas;
    - Environmental or industrial exposure to arsenic, chromium, chloromethyl ether, vinyl chloride and polycyclic aromatic hydrocarbons;
    - Genetic predisposition
  - ▪ Other disorders of respiratory system : hypoxia, asphyxia, bad cold, bronchitis, bronchial asthma, pneumonia, emphysema, occupational respiratory disorder, carbon monoxide poisoning;
  - ▪ Throat cancer and ENT
- ♦ Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];
- ♦ Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
- ♦ Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
- ♦ Estimate requirements of healthcare in terms of demand plan (P^p_d);
- ♦ Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
  - ▪ Auto-immunity and vaccination;
  - ▪ Optimal diet intake to fight against malnutrition;
  - ▪ Life-style : Avoid smoking and alcohols, food habit, drug addiction control, obesity and overweight control, yoga (deep breathing exercises) and physical activities, stress control through meditation;

Reactive approach:

- adopt sense-and-respond strategy.
- assess risks of single or multiple attacks on the human respiratory system; analyze performance, sensitivity, trends, exception and alerts.
  - ♦ what is corrupted or compromised?
  - ♦ time series analysis : what occurred? what is occuring? what will occur?
  - ♦ insights : how and why did it occur? do cause-effect analysis.
  - ♦ recommend : what is the next best action?

        - **predict: what is the best or worst that can happen?**
- **verify security intelligence of application, computing, networking, security and data schema of biological system.**
    - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**
    - **Level 2: authentication, authorization, correct identification, privacy, audit;**
    - **Level3: safety, reliability, consistency, liveness, deadlock freeness, reachability, resiliency;**
    - **Level4: stability, system dynamics, quality of application integration.**
- **Explore risk mitigation plan.**
    - **Prevention measures of lung cancer : stop smoking , early detection and screening and chemoprevention;**
    - **Do medical testing of data schema (^);**
    - **Data visualization of X-ray report of lungs and also biopsy report;**
    - **Treating tobacco induced injuries in the air way, viral and bacterial infection, chronic inflammation; medication against chronic disease;**
    - **Limited disease of lung cancer (LD) :**
        - **combined chemo radiation therapy**
            - **radiation intensity**
            - **timing of chemotherapy : Sequential, concurrent, and alternating chemotherapy**
        - **surgery**
    - **Extensive disease of lung cancer (ED):**
            - **Select correct treatment algorithm**
            - **systematic chemotherapy**
            - **immunotherapy through tumor vaccines**
- **Fight against bad luck : Identify critical risk elements.**
    - **Genetic disorder**
    - **Reproductive disorder (flaws in organ formation and development since birth)**
    - **Injuries from accidents, war and crime**
    - **Occupational exposure**
    - **Air and soil pollution**
    - **Hostile climate, weather and other locational disadvantages, exposure to sunshine, snowfall and very cold climate;**
    - **Malnutrition due to poverty**
- **Develop risk mitigation plan in terms of surgical operation and migration of human civilization from risky zone.**

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

F. Body fluids circulation – Cardiovascular system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human biological system – (a) body, (b) mind;
Objectives: cancer prevention at optimal cost; focus : leukemia or blood cancer [29,30];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- ♦ **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
  - **Identify targets**
    - ♦ **application schema : cardiovascular system;**
    - ♦ **networking schema : heart, blood vascular system – open and closed circulatory system, arterial and venous system, blood, tissue fluid, lymphatic system – spleen, thymus, tonsils;**
    - ♦ **computing schema : pulmonary and systemic circulation, blood clotting or coagulation mechanism, blood flow mechanism;**
    - ♦ **data schema : blood group, efficiency of heart, heart rate, heart output, pulse, heart sound;**
    - ♦ **security schema : blood, lymph, water, minerals, vitamins, hormones;**
  - **Threat modeling**
    - ♦ **Call threat analytics and assess miscellaneous risk elements :**

        - **blood cancer / lukemia**
            - **Acute lymphoblastic leukemia (ALL) : proliferation and accumulation of lymphoid progenitor cells in blood, bone marrow and tissues for both the children and adult; bone marrow failure, malaise, fatigue, bleeding fever, night sweats, weight loss and abnormal White blood cell (WBC) count;**
            - **Adolescent and young adult acute lymphoblastic leukemia;**
            - **Acute myeloid leukemia (AML) due to genetic mutations and chromosomal aberrations with symptom of Fanconi anemia;**
            - **Chronic lymphocytic leukemia (CLL): clonal hematopoietic disorder;**
            - **Chronic myeloid leukemia (CML)**
        - **blood pressure disorder (SP, DP)**
        - **cardiovascular diseases : Stroke (CVA or cardiovascular accident), rheumatic heart disease (RHD), coronery artery disease (CAD), hypertensive heart disease, atrial fibrillation, tachycardia, vaculities;**
    - ♦ **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
    - ♦ **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
    - ♦ **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**
    - ♦ **Estimate requirements of healthcare in terms of demand plan (P^p_d);**
    - ♦ **Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.**
        - **Auto-immunity and vaccination**
        - **Optimal diet intake to fight against malnutrition**
        - **Life-style : Avoid smoking and alcohols, food habit, drug addiction control**

- **Reactive approach:**
    - **adopt sense-and-respond strategy.**
    - **assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.**
        - ♦ **what is corrupted or compromised?**
        - ♦ **time series analysis : what occurred? what is occuring? what will occur?**
        - ♦ **insights : how and why did it occur? do cause-effect analysis.**

        - **recommend : what is the next best action?**
        - **predict: what is the best or worst that can happen?**
    - **verify security intelligence of application, computing, networking, security and data schema of biological system.**
        - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**
        - **Level 2: authentication, authorization, correct identification, privacy, audit;**
        - **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**
        - **Level4: stability, system dynamics, quality of application integration.**
    - **Explore risk mitigation plan (P^r_d and P^r_m).**
        - **Diagnosis of ALL: immunophenotyping, cytogenetic-molecular profiling, allogeneic stem cell transplantation, salvage therapy, immunotherapy*;***
        - **Risk stratification of AML based on patient related variables (age and performance) and disease related predictors (cytogenetic and molecular characteristics);**
        - **Induction therapy, supportive care and stem cell transplantation for AML;**
        - **Do medical testing → Data visualization of ECG**
        - **Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance**
        - **Medication for blood pressure control**
        - **Integrated medicine**
        - **Regenerative medicine**
- **Fight against bad luck : Identify critical risk elements.**
        - **Genetic disorder (sex, race, ethnicity, somatic mutation)**
        - **Reproductive disorder (personal, hormonal and family history)**
        - **Occupational exposure**
        - **Air, water and sound pollution**
        - **Hostile climate, weather and other locational disadvantages, exposure to sunshine**
        - **Malnutrition due to poverty**
    - **Develop risk mitigation plan in terms of organ transplantation, surgical operation, blood substitution and migration of human civilization from risky zone.**

Payment function:

- **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**

- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

G. Excretory system

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human excretory system;
Objectives: cancer prevention at optimal cost; focus : renal cancer, skin cancer [31];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- ♦ **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
    - **Identify targets**
        - ♦ **application schema : excretory system;**
        - ♦ **networking schema : kidney - nephron, ureters, urinary bladder and urethra; skin – sweat, lungs – CO_2;**
        - ♦ **computing schema : urea and urine formation, mechanism of kidney;**
        - ♦ **data schema : urine and stool – quantity, physical properties, chemical composition and renal threshold;**
        - ♦ **security schema : immunity, water, vitamins, minerals;**
    - **Threat modeling**
        - ♦ **Call threat analytics function and assess various risk elements :**
            - ▪ **renal cancer : tobacco smoking, regular alcohol consumption, food habit (e.g. high intake of animal protein and fat), polluted drinking water, obesity, lack of physical activities, reproductive factors and hormones, medical conditions : hypertension, diabetes, urinary tract disease, drug addiction, radiation , occupational exposure : chemical, oil and**

    gas, Pb, Cd, asbestos, gasoline and hydrocarbons, genetic susceptibility;

- **kidney disorder - renal failure, kidney stone; uremia, cystitis, glomerrulonephritis, pyelonephritis;**
- **urinary bladder cancer**
- **prostate cancer**
- **skin cancer : actinic keratosis, melanoma skin cancer, non-melanoma skin cancer;**

- **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
- **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
- **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**
- **Estimate requirements of healthcare in terms of demand plan $(P^p{}_d)$;**
- **Explore risk mitigation plan $(P^p{}_m)$: accept / transfer / remove / mitigate risks.**
    - **Auto-immunity and vaccination;**
    - **Optimal diet (e.g. fruits, vegetables) and water intake to fight against malnutrition;**
    - **Life-style : Avoid smoking and alcohols, food habit (e.g soft drinks), drug addiction control, wild polygamy, obesity and overweight control through yoga and physical activities;**

- **Reactive approach:**
    - **adopt sense-and-respond strategy.**
    - **assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.**
        - **what is corrupted or compromised?**
        - **time series analysis : what occurred? what is occuring? what will occur?**
        - **insights : how and why did it occur? do cause-effect analysis.**
        - **recommend : what is the next best action?**
        - **predict: what is the best or worst that can happen?**
    - **verify security intelligence of application, computing, networking, security and data schema of biological system.**
        - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**
        - **Level 2: authentication, authorization, correct identification, privacy, audit;**
        - **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**

  - Level4: stability, system dynamics, quality of application integration.
- Explore risk mitigation plan.
  - skin cancer :
    - actinic keratosis – cryotherapy, topical treatment;
    - melanoma skin cancer : biopsy – shave, punch, excisional, incisional, wound care;
    - non-melanoma skin cancer : topical treatment, ED&C, excision, radiotherapy;
  - renal cancer: immunotherapy, radiotherapy and supportive care, systemic therapy of metastatic disease, adjuvant therapy, surgical treatment of renal cell carcinoma, interventional radiology, laparoscopic radical nephrectomy;
  - Do medical testing → Data visualization of kidney scan (Refer Deep Leaning Algorithm of section 5.1, transferring a Convolutional Neural Network, trained on images for detection of kidney problem in ultrasound images); detection of renal tumor by USG, MRI and CT scan;
  - Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;
  - Artificial kidney or kidney transplantation
  - Integrated medicine
- Fight against bad luck : Identify critical risk elements.
  - Genetic disorder (sex, race, ethnicity, somatic mutation)
  - Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)
  - Injuries from accidents, war and crime
  - Occupational exposure
  - Water pollution
  - Hostile climate, weather and other locational disadvantages,
  - Malnutrition due to poverty
  - Develop risk mitigation plan in terms of organ transplantation and surgical operation and migration of human civilization from risky zone.

Payment function:

- Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.
- Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.
- Trade-off proactive vs. reactive security; assign weights to each approach.

- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

H. Locomotion and Movement

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human biological system – (a) body, (b) mind;
Objectives: cancer prevention at optimal cost; focus: bone cancer [32,33];
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender : The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- ♦ **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- ✚ **Proactive approach:**
    - **Identify targets :**
        - ♦ **application schema : human skeletal and mascular system;**
        - ♦ **networking schema :**
            - ▪ **skeleton – bone (skull, spinal column, ribs, sternum, girdles, limb), cartilage, joints;**
            - ▪ **muscles – red and white;**
        - ♦ **computing schema :**
            - ▪ **Mechanism of metastasis to bone, inflammatory cytokines in osteolysis, prostate cancer bone colonization causing metabolic imbalance between osteoblasts and osteoclasts, tumor-bone interaction, suppression of bone formation;**
            - ▪ **locomotion and movement mechanism, autonomic and induced movement,**
            - ▪ **muscle contraction mechanism;**
        - ♦ **data schema : oxygen debt, muscle fatigue;**
        - ♦ **security schema : bone marrow, minerals, vitamin D;**
    - **Threat modeling**
        - ♦ **Call threat analytics and assess miscellaneous risk elements :**
            - ▪ **Risk factors : age, gender, race, site distribution;**
            - ▪ **bone cancer : bone pain, spinal chord suppression;**
            - ▪ **osteosarcoma (primary and malignant bone tumor);**

        - multiple myeloma : bone destruction, hypercalcemia, neurological disorder;
        - head and neck cancer, cervix cancer ;
        - Other disorders: sprain, arthritis, osteoporosis, dislocation, slipped disc, fracture of bones, bursitis, tetany, myasthenia gravis and muscular dystrophy.
    - Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];
    - Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];
    - Map threats into a set of risk profiles or classes : LL, LH,HL and HH;
    - Estimate requirements of healthcare in terms of demand plan (P^p_d);
    - Explore risk mitigation plan (P^p_m) : accept / transfer / remove / mitigate risks.
        - Auto-immunity and vaccination;
        - Optimal diet intake to fight against malnutrition;
        - Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control;
        - Fairplay : Take less risk in sports, games and adventure;
        - yoga and physical mascular activities, stress control through meditation;
        - Use computers, tablets and laptops with a safe posture.

- **Reactive approach:**
    - adopt sense-and-respond strategy.
    - assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.
        - what is corrupted or compromised?
        - time series analysis : what occurred? what is occuring? what will occur?
        - insights : how and why did it occur? do cause-effect analysis.
        - recommend : what is the next best action?
        - predict: what is the best or worst that can happen?
    - verify security intelligence of application, computing, networking, security and data schema of biological system.
        - Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;
        - Level 2: authentication, authorization, correct identification, privacy, audit;

- ♦ **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**
- ♦ **Level4: stability, system dynamics, quality of application integration.**

- **Explore risk mitigation plan .**
    - ♦ **Bone cancer treatment : radio graphy, radio surgery, bone marrow transplant, treatment against side effects of hormonal therapy in breast and prostate cancer, bone pain management;**
    - ♦ **Bone pain management through eradication of bone tumors, decreasing the impact of tumor induced bone loss, surgical stabilization of fractures and pain medications;**
    - ♦ **Optimal therapy and treatment outcomes in head and neck cancer through precise identification of the primary tumor and also local, regional, and distant extent of disease.**
        - ▪ **Combined modality therapy**
            - **Induction chemotherapy**
            - **Concomitant radiotherapy and chemotherapy**
            - **Adjuvant Chemoradiotherapy**
    - ♦ **Do medical testing → Data visualization of digital x-ray, molecular images of cancer cells growing in bones, detection of tumor cells in bone marrow;**
    - ♦ **Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;**
    - ♦ **Physiotherapy**
    - ♦ **Integrated medicine**

- ✚ **Fight against bad luck : Identify critical risk elements.**
    - ♦ **Genetic disorder (sex, race, ethnicity, somatic mutation)**
    - ♦ **Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)**
    - ♦ **Injuries from accidents, war and crime**
    - ♦ **Bone fracture in sports and games (e.g. football, rugby, boxing)**
    - ♦ **Occupational exposure (e.g. mason)**
    - ♦ **Environmental pollution**
    - ♦ **Hostile climate, weather and other locational disadvantages;**
    - ♦ **Malnutrition due to poverty**
  - **Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.**

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan

I. Reproductive System

Agents: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);
Model: Human reproductive system;
Objectives: cancer prevention at optimal cost; focus : (a) ovarian cancer; (b) testicular cancer;
Constraints: budget or financial constraint, resources, time, knowledge;
Input: Perception of human agent, performance measures of biological system or test data;
Strategic moves: deep learning, intelligent reasoning (perception, analytical, logical, common sense), optimal mix of proactive and reactive approaches, rational healthcare payment function and budget plan, adaptive secure multi-party computation;
Revelation principle: The agents preserve privacy of strategic data;

- ♦ **Defender: The defenders share critical information collaboratively – collaborative planning, treatment and exception management (CPTEM).**
- ♦ **Attacker: The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

Cancer Prevention Approaches:

- **Proactive approach:**
  - **Identify targets :**
    - ♦ **application schema : human reproductive system;**
    - ♦ **networking schema :**
      - ▪ **male : scrotum, testes, vasa efferentia, epididymes, vasa deferntia, ejaculatory ducts, urethra, penis; prostate glands;**
      - ▪ **female : ovaries, fallopian tube, uterus, vagina, vulva, breast;**
    - ♦ **computing schema : spermatogenesis, oogenesis, menstrual cycle, menopause, fertilization, cleavage, implantation, gastrulation, organogenesis, parturition, lactation;**
    - ♦ **data schema : sperm, ovum, egg, zygote;**
    - ♦ **security schema : hormones, minerals, vitamins;**
  - **Threat modeling**
    - ♦ **Call threat analytics and assess miscellaneous risk elements :**

        - **Testicular cancer**
            - **Metastatic germ cell cancer**
            - **CSI Non-seminoma**
        - **Ovarian cancer**
            - **genetic risk factors : inherited susceptibility,**
            - **hormonal risk factors (estrogen and progesterone)**
            - **age at menarche and age at menopause, gender, race**
            - **pregnancy, parity and infertility**
            - **lactation, benign gynecologic conditions and gynecologic surgery**
            - **oral contraceptives**
            - **hormone replacement therapy**
            - **anthropometric factors**
            - **diet and nutrition, lack of exercise and physical activity, life-style and environmental factors : smoking, alcohol consumption, asthma, drug use, occupational exposure**
        - **other disorders : impotence, sterility, menstrual irregularity, prostetomegaly;**
    - **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
    - **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
    - **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**
    - **Estimate requirements of healthcare in terms of demand plan;**
    - **Explore risk mitigation plan : accept / transfer / remove / mitigate risks.**
        - **Auto-immunity and vaccination;**
        - **Optimal diet intake to fight against malnutrition;**
        - **Life-style : Avoid smoking and alcohols, food habit, drug addiction control, wild polygamy, obesity and overweight control;**
        - **yoga and physical activities, stress control through meditation;**
        - **secure multi-party computation**

- **Reactive approach:**
    - **adopt sense-and-respond strategy.**
    - **assess risks of single or multiple attacks on the human biological system; analyze performance, sensitivity, trends, exception and alerts.**
        - **what is corrupted or compromised?**
        - **time series analysis : what occurred? what is occuring? what will occur?**

  - **insights : how and why did it occur? do cause-effect analysis.**
  - **recommend : what is the next best action?**
  - **predict: what is the best or worst that can happen?**
- **verify security intelligence of application, computing, networking, security and data schema of biological system.**
  - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**
  - **Level 2: authentication, authorization, correct identification, privacy, audit;**
  - **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**
  - **Level4: stability, system dynamics, quality of application integration.**
- **Explore risk mitigation plan.**
  - **Testicular cancer**
    - **USG detecting a painless swollen mass in testes**
    - **Determination of AFP, LDH and hCG**
    - **Surgical exploration in testis to detest germ cell tumor**
    - **Orchiectomy**
    - **Organ preserving surgery in case of benign histology**
    - **Surveillance for low risk patients and adjuvant BEP chemotherapy for high risk patients and also risk adapted treatment**
    - **First line treatment for metastatic disease and residual tumor resection**
    - **Salvage treatment, late relapse and follow up**
    - **Treatment of fertility and sexuality : hypogonadism, ejaculatory disorder, disorder with erectile function and libido, metabolic syndrome (MBS)**
  - **Ovarian cancer:**
    - **screening and early detection,**
    - **early stage treatment : staging, adjuvant chemotherapy,**
    - **advanced stage treatment : surgical debulking principle,**
    - **chemotherapy for recurrent ovarian cancer;**
    - **targeted molecular therapy (TMT)**
  - **Treating viral and bacterial infection, chronic inflammation, pain, diabetes, cholesterol and hormonal imbalance;**
  - **Radiotherapy**
  - **Integrated medicine**

- **Fight against bad luck : Identify critical risk elements.**

        - ♦ **Genetic disorder (sex, race, ethnicity, somatic mutation)**
        - ♦ **Reproductive disorder (flaws in organ formation and development since birth, personal, hormonal and family history)**
        - ♦ **Occupational exposure (e.g. high workload, stress)**
        - ♦ **Environmental pollution**
        - ♦ **Hostile climate, weather and other locational disadvantages**
        - ♦ **Malnutrition due to poverty**
    - **Develop risk mitigation plan in terms of organ transplantation, surgical operation, and migration of human civilization from risky zone.**

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in healthcare.**
- ♦ **Trade-off proactive vs. reactive security; assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Cancer prevention plan.

SESSION 6: ENERGY & UTILITIES SECURITY for HUMANITY - SOLAR POWER ELECTRONICS, NANO SOLAR CELL, INDUCTION COOKER

Event **: Technology for humanity and global security summit**
Venue**: Energy & utility security hall, Technology park : Sanada**
Time **Schedule : 10 a.m.. – 1 p.m. , 16.8.2020**
Agents **: Representatives of various global organizations (UN, UNICEF, UNESCO,WHO, World bank, Global Economic forum), Technology management experts from science and technology forums on renewable energy, Environmental engineers, Climate change and social activists, Social scientists, representatives and ministers from the departments of energy and utilities of developed, developing and underdeveloped countries, CEOs of solar power companies, business development consultants of wnergy and utilities sectors, Engineers and scientists of electrical, electronics, power plant, chemical engineering.**
Topic of discussion and key focus areas **: Energy security, Utilities security, Solar power, Solar induction cooker, Solar power electronics, Nano solar cell, Deep Analytics, Business model innovations, Solar microgrid, Technology diffusion, SWOT analysis Pure drinking water supply, Mobile communication.**
Keynote speakers **: Dr. Paolo Maradona, Prof. Bruno Platini, Prof. Tony Fergunson, Prof. Johan Macacini, Dr. Robert Messi.**

1. SCOPE

Scope Analytics

Agents**: system analysts, business analysts; scientists;**
Moves **: Critical success factors analysis, Requirements management;**
Security parameters**: define a set of sustainable development goals.**

- ***Energy security*** **: clean and affordable power;**
- ***Utilities security*** **:**
  - **pure drinking water : artificial rain, water conservation /* refer to session 2*/**
  - **oil (petrol, diesel) /* refer to session 7*/**
  - **gas: solar induction cooker may be a substitute of gas for cooking application;**
  - **telecom /* refer to session 8*/**
  - **internet /* refer to session 8*/**
  - **computing /* refer to session 8*/**
- ***Poverty control***
- ***Business model innovation***
- ***Environmental pollution control***

Application domains **: Solar lighting system, solar power pack, consumer electronics and home appliances, solar water heater, solar charging for computing devices and**

mobile phones, solar water pumps for agriculture, solar induction cooker, solar microgrid for rural electrification.

Prof. Tony Fergunson and Dr. Robert Messi have started the session exploring various applications of solar power system. The issues of water, oil (petrol, diesel) and telecom, computing and internet have been covered during sessions 2, 7 and 8 respectively. Entrepreneurial success depends on various factors. The *critical success factors* are associated with entrepreneurial motivation, creativity, business model innovation, rational and intelligent business plan, core competencies, new technology management, sustainable policy for economic growth, corporate social responsibilities, industry structure, government's support in terms of incentives and subsidies, dynamic role of entrepreneurial education institutes, business incubator, business cluster and good support of financial institutions. Let us first explore a set of innovative business models for solar power technology.

This session is focused on the problem of global energy security and has explored a set of fundamental research agendas: What should be the strategic moves for the diffusion of solar technology? What should be the dominant design of solar power system in terms of structure and security? What is the scope of solar technology? What should be the right innovation model? What is the outcome of a rational SWOT analysis on various types of energy? What is the outcome of solar technology life-cycle analysis? Solar power electronics and nanotechnology based solar cells are two critical success factors of the dominant design of solar power system for the improvement of energy conversion efficiency and reduction of cost of solar energy generation. Are there any other interesting strategic moves in this connection? Is it really possible to enhance the absorption capacity of solar cells by 1000 times using the concept of nanotechnology? Can we adopt K-A-B-C-D-E-T-F innovation model for fast diffusion of solar technology globally?

Photovoltaic (PV) is the most direct way to convert solar radiation into electricity and is based on the photovoltaic effect, which was first observed by Henri Becquerel in 1839. Solar power electronics is an interesting option in transformation of old and traditional energy system which requires fundamental rethinking and radical redesign of as-is energy policy and technology. The present work has analyzed the technology of solar power through deep analytics in terms of seven 'S' dimensions: scope (S_1), system (S_2), structure (S_3), security (S_4), strategy (S_5), staff-resources (S_6) and skill-style-support (S_7). Effective solar technology diffusion strategy demands a perfect fit, proper coordination and integration among these seven elements. It is clear from scope and SWOT analysis that solar power is a potential option of sustainable energy and business model innovations for the future as compared to other sources of energy. There are some technological constraints such as efficiency and cost of solar cells. Presently, solar power system is at the growth phase of technology life-cycle and it demands an intelligent and rational technology diffusion strategy through the support, commitment and involvement of efficient and creative innovators.

The basic objective of this session is to analyze the technology of renewable energy, more specifically solar energy. This is an interesting cross-fertilization between management science (e.g. business intelligence, technology management,

entrepreneurship) and engineering science (e.g. photonics, power electronics, chemical engineering, electrical engineering, renewable energy and structural engineering). It is basically a modest effort to business model innovation and system implementation; it tries to explore a set of fundamental questions based on rational analytics: What are the intelligent moves in solar technology management? Who are the customers? What do they value? How is it possible to deliver value to the customers at optimal cost? What are the emerging application domains? What is the revenue model? What is the quality policy? What are the corporate social responsibilities? Can the business model generate significant number of new job opportunities in our society? Is the technology ready, feasible and practically implementable? What are the major constraints? What are the critical success factors?

The contribution of this work is that proper diffusion of solar technology at a fast speed requires effective coordination and integration among seven 'S' elements of the deep analytics. These moves must be integrated, coordinated and synchronized for effective diffusion of solar power technology. The scope analytics outline a set of interesting business model innovation in solar technology. The system intelligence is explored along five dimensions: smart materials innovation for photonic cell, power electronic circuit intelligence in terms of power amplifier, DC-DC boost converter, microinverter, energy storage, energy efficient load (e.g. LED, computing devices, motors) and topology (e.g. microgrid, standalone or hybrid system). The security intelligence is explored along four dimensions: switchgear, relay and earthing system and maximum power tracking based load manager. The strategic intelligence is associated with good governance, good wishes in public policy, industry analysis, efficient enterprise resource planning, supply chain management and marketing efforts like strategic pricing, promotion, trust in communication, sales and distribution.

The business model requires the support of a functional organization structure enabled with advanced information and communication technology. The structure should have project, power generation, distribution, maintenance, revenue management, HR, SCM and finance cells. The structure is also important for effective knowledge management: creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The business model should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated staffs or HR workforce.

The workforce require different types of skills such as research and development, product design, sales, event management, project management, erection, testing, commissioning and service maintenance. One of the critical success factors is the style or quality of leadership in terms of motivation, commitment, support, coordination and excellent communication. The leaders must be able to share vision and values among all the stakeholders honestly and appropriately in time. It is really challenging to implement the solar power system physically and practically for global energy security. There are different threats from traditional industries: coal, oil and gas, thermal and nuclear power, local bias, power play and politics. It is essential to understand the intelligence of business modeling and system dynamics, fundamental rethinking and radical redesign of global energy trading. The

traditional boundaries of electrical, power and consumer electronics and structural engineering industries must be redefined for future growth in a stable way. The research methodology adopted for this work includes literature review on solar energy, photonics and photovoltaic power electronics and case analysis.

The people of today's world need energy security through emerging renewable technology, new business models and innovative applications. Presently, the global energy consumption is 10 TW per year and 30 TW by 2050. The solar energy plays a significant role in meeting the global energy demand in future. Solar power is useful for the growth of rural, urban, semi-urban and remote zone. The business models based on solar power can create significant number of new job opportunities in photovoltaic micro grid project, erection, installation, testing, commissioning and maintenance of standalone solar power system. Further, there are good opportunities of technology consulting in power electronics and product design and business consulting in global supply chain management. This section explores various types of innovative business models and applications of solar power electronics in terms of solar lighting system, solar power pack, consumer electronics and home appliances, solar charging for laptop and tablets, microgrid for rural electrification and solar water pumps for agriculture with some practical examples of business analytics. This section requires detailed cost benefit analysis based on current technical and commercial data.

***Solar Lighting System* : Solar power system can be used intelligently in various applications such as lighting of homes, religious places, tourist spots, streets, transportation management systems (e.g. airport, rail stations, bus stops, public toilets), educational institutes (e.g. schools, colleges, universities, research labs), healthcare institutes (e.g. public and private hospitals, health clinics, drug shops, pathological lab), office buildings of public and private firms, IT firms, hotels, restaurants, dairy firms, biotechnology firms and food processing units and space science. A typical solar lighting system can illuminate a house of 5 persons lighting 5 lamps for up to 5 hours daily. It can save the cost of 300 litres of Kerosene of about Rs. 10,000. The PV panel converts solar radiation into electrical power; the current is controlled by a charge controller or inverter and charges a battery. The battery supplies power to the connected load while switched on and illuminate. Rooftop solar power system should be used as alternative power supply during power cut due to cyclone or other various types of disaster.**

***Solar Power Pack*: A power pack consists of a set of solar panels which convert solar radiation into electrical energy and transmit the power to domestic load or battery bank through a smart inverter. The battery bank stores surplus power when the demand mismatches with the supply. The inverter interacts with PV panel, domestic load, grid and battery intelligently to ensure continuous and regular supply of power. The rating may vary between 100W upto a few KW. A 1 KW power pack can save fuel cost of Rs. 50,000 per annum approximately and can also save energy bill of Rs. 10000 per annum.**

***Consumer Electronics and Home Appliances:* Solar cells can be used as economical power supplies with miscellaneous applications such as solar cookers, fans, mobile phones, watches, tablets, laptops, torches, emergency lamps, LED, calculators,**

radios, televisions, freezes, air conditioners, water heaters, cars and other different types of home appliances. Solar cells are generally used in *space vehicles*.

Solar water heater: **A solar water heater consists of a collector, pipes and an insulated tank. The collector is made of glass tubes in evacuated vacuum tube system or metallic tubes in flat plate collector system. It gets heated in sunlight and the heated water reaches the top of a water tank. The relatively colder and denser water descends into the tubes and gets heated through a continuous Thermo-siphon cycling effect. A 100 LPD water heater provides 100 litres of hot water at 65°C and saves Rs. 5000 energy cost annually. The existing design needs a change in terms of mechanism, size and compactness. Solar power enable water purifier is expected to be attached with tube wells in urban and rural zone to ensure the supply of clean purified drinking water.**

Solar Charging for Computing Devices and Mobile Phones: **Solar charging of batteries has recently become very popular for laptops, tablets and mobile phones. The typical voltage output of a solar cell is 0.7 V. A solar panel may have eight cells connected in series producing 5.6 V at most. It can charge a single Li-ion battery used in cell phones to 4.2 V with a buck or step-down charger. It requires a boost step-up charger to charge a multicell Li-on battery of a laptop.**

Solar Water Pumps for Agriculture : **The expert panel have already discussed the application of solar water pumps for agriculture during session 3 [58,59].**

Solar induction cooker **[53-57]*: Solar cooker* is an interesting emerging application; it may be a direct or indirect application. An indirect application is related to the use of induction cooker or microwave oven enabled with solar panel. Let us exercise SWOT analysis of solar induction cooker and conventional gas cooking oven / gas pipelines. Is it possible to explore the option of solar power enabled induction cookers at mass scale? Solar power enabled induction cooker should be a substitute of costly cooking gas. It is irrational to invest capital on new gas pipeline projects today in the age of induction cooker. Solar cooker uses the solar energy from direct sunlight to heat, cook or pasteurize food or drink. It is relatively inexpensive, reduces fuel cost, having simple technology and large solar cookers can cook for hundreds of people. Solar cookers have various advantages in terms of minimal fuel consumption, reduced danger of accidental fire, health and environmental pollution.**

There are many types of solar cookers such as parabolic, solar ovens and panel cookers. The basic principle of solar cooker is based on concentration of sunlight, conversion of light into heat and trapping of heat. A mirrored surface with high reflectivity concentrate sun light on a small cooking area. It can produce high temperature like 65 - 400°C depending on the geometry of the surface. An alternative design of solar cooker concentrates sunlight on a receiver such as a cooking pan. The interaction between solar energy and the receiver material converts light to heat; it is maximized by materials which can conduct and retain heat. The convection of heat can be reduced by isolating the air inside and outside the cooker. Parabolic solar cookers concentrate sunlight to a single point which is focused on the bottom of a pot and can heat the pot quickly to very high temperature. Parabolic troughs are used to concentrate sunlight for solar-energy. Spherical reflectors operate like paraboloidal reflectors and can attain temperatures

above 290°C to cook meat, vegetable, soup, baking of bread and boiling water in minutes.

But, solar cookers are less useful in cloudy weather and near the poles and may take longer time to cook food. The alternative solution is the adoption of induction cooker which can be operated through solar power fed by PV panels. It is essential to design user friendly solar cooker which can be commercialized. The basic principle is to incorporate heating into material by photovoltaic effect and thermal treatment. An efficient solar cooker needs the boosting of only 30W which is generated by a small standalone solar panel of 75W.

***Solar Microgrid for Rural Electrification:* A smart *Microgrid* is an interesting option of rural electrification [Figure 6.1]. It consists of solar panels, power condition unit (PCU), distribution box (DB), battery system and loads. Its size depends on the load estimation and the number of PV panels and rating of solar cells. The PV panels comprise of a set of solar cells connected in series or parallel; they convert solar radiation into electrical power; the power flows from PV panels to PCU or power inverter; PCU controls, regulates and directs the power to various loads (e.g. domestic load, water pumps in Greenfield). The surplus power generated in the daytime is stored in the battery bank and may be utilized after the sunset. The typical energy demand of a rural house is approximately 3 units. For a village of 100 houses, a 5 KW microgrid may be useful. It can generate annual energy of Rs. 50000. It is an approximate calculation.**

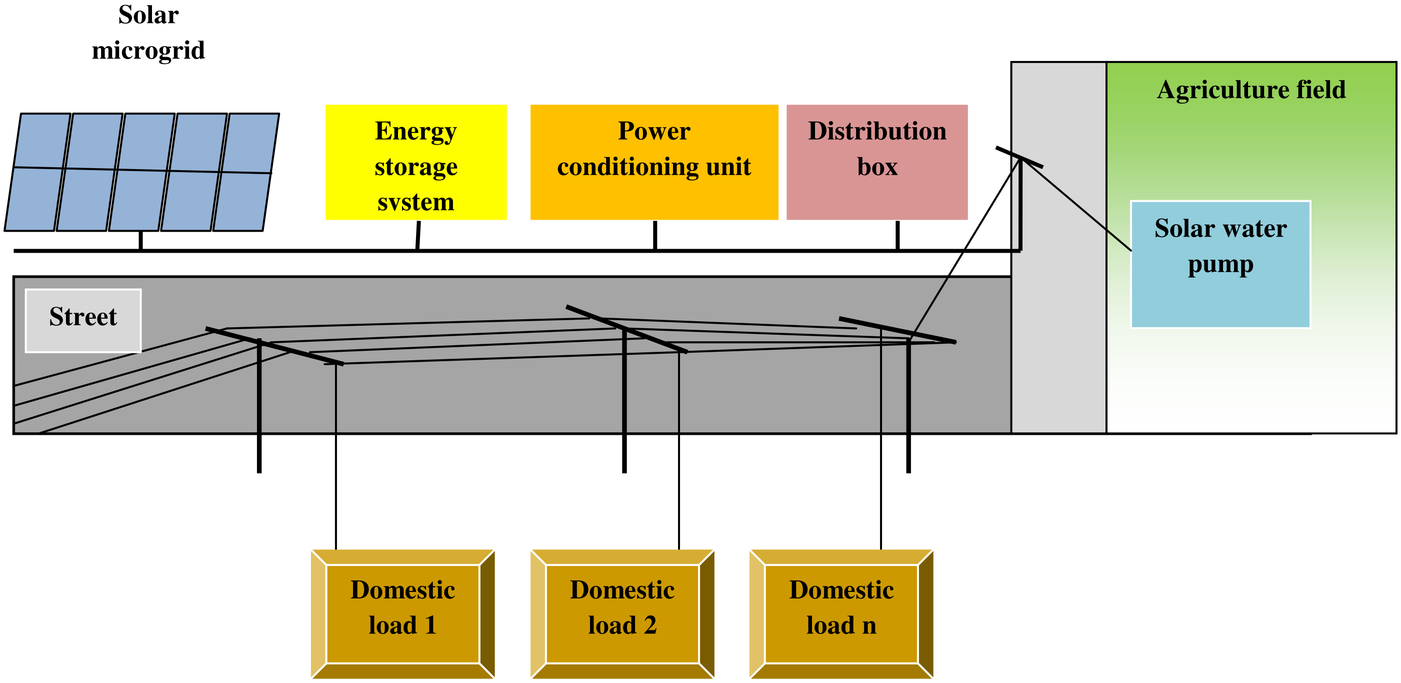


Figure 6.1: Solar microgrid for rural electrification

Let us consider the application of solar power for rural electrification: how solar power can illuminate the life of poor rural people. The innovative business model of solar power can save energy cost of rural people in domestic applications and agriculture. The peasants and farmers can reduce the cost of energy used in water pumps for irrigation in agriculture. It can improve the productivity required for green revolution. Many rural people suffer from road accidents and snake bites due to lack of adequate street light; the solar power can save them from those dangers in the form of solar torch. The rural students can study in the evening and night effectively using solar lamps. The rural people can save the cost of energy used for home appliances and domestic power supply. They are able to use modern electrical and electronics systems (e.g. home appliances, TV, music system, mobile phones, i-pod, computers, laptops, washing machines, freeze, induction cookers, microwave ovens etc.) through the use of solar power economically. In summer, they can feel comfortable using fans and air-conditioners and in winter, they can use room heaters and geezers. Rural market is a potential option for the growth of consumer electronics and electrical industries.

PV Panels or Solar Cells Manufacturing: **The present global PV market is growing at about 40% per year and global PV production was about 11 GW in 2009 due to rapid reduction in production cost, technology improvement and market development reflecting the economy, reliability and versatility of solar energy. About 80% of the global PV production is based on c-Si and pc-Si wafer technologies. Major market segments comprise consumer applications, industrial systems, rural electrification in developing countries, microgrid and hybrid systems. The major markets exist in USA, European Union (e.g. Germany), Japan, China and Taiwan. The top ten producers of PV cells and modules are First Solar, Suntech Power, Sharp, Q-cells, Yingly Green Energy, JA Solar, Kyosera, Trina solar, Sunpower and Gintech. In future, a set of PV panels (or solar cells) manufacturing plants should be set up in India through joint ventures. Definitely, the new industrial units will be able to boost the growth of manufacturing industry in India.**

The budding entrepreneurs must try to explore a set of fundamental questions based on rational analytics: Who are the customers? What do they value? How is it possible to deliver value to the customers at optimal cost? What are the emerging application domains? What is the revenue model? What is the quality policy? What are the corporate social responsibilities? Can the business model generate significant number of new job opportunities? Is the technology ready, feasible and practically implementable? What are the major constraints? What are the critical success factors? What are the business intelligence moves in solar technology management? How to make an effective business plan? What are the critical elements of an intelligent business plan? A good business model consists of four interlocking elements : customer value proposition in terms of target customers, jobs and product and service offerings; profit formula in terms of revenue model, cost structure, margin model and resource velocity; key resources such as people, technology, products, equipments, information, channels, partnerships, alliances and brand and key processes, rules, metrics and norms. A good business plan must have a set of common elements such as executive summary, the mission and vision of a company, organization structure, roles and responsibilities of management team,

industry analysis, market, operation management strategy, marketing plan, financial plan, risks assessment and mitigation strategy. Many ventures fail due to lack of intelligence in defining a good business model and business plan.

The entrepreneurs need the support of business incubator, social network, business cluster and single window system from the ministry of MSME (Micro, Small and Medium enterprises). Entrepreneurial development institutes and MSME training institutes should focus on developing entrepreneurial skills in the domain of solar power electronics. A business incubator can nurture new ventures by providing them good guidance and support during start-up period. The entrepreneurs also need good network of technical experts and business development consultants. A business cluster may gain performance advantage through co-location, business relationships, right infrastructure and right skills. The aspiring entrepreneurs should be able to get all necessary permits and clearances by applying to a single agency of MSME ministry. The ministry of MSME should offer value adding incentive schemes and good mechanisms for access to debt, equity and venture capital, tax breaks, stimulating innovation, access to market and simplification of administrative burden and legal hassles. The policies should be correctly evaluated on regular basis. The rural banks and cooperative banks should launch innovative schemes (e.g. loan guarantee) to fulfill the needs of the budding entrepreneurs for rural electrification though smart Microgrids. Finally, the budding entrepreneurs must have commitment, determination, patience, tolerance of risk and uncertainty, creativity, self-reliance and motivation for successful ventures on solar power electronics.

3. SYSTEM

System Analytics

***Agents*: system analysts, business analysts, scientists, engineers of renewable technology, electrical and electronics technology forum;**

***Objects* : sustainable smart cities, smart villages;**

***Moves* : requirements engineering, system design, prototype testing, erection, installation, testing, commissioning**

***System intelligence* : Innovate a set of emerging technologies related to solar power;**

- **Photonic cell : Nano PV;**
- **Power electronics : DC-DC boost converter, Inverter;**
- **Topology : solar microgrid, standalone system, hybrid system;**
- **Energy efficient load : LED light;**
- **Battery storage;**

Prof. Bruno Platini is giving a presentation on the emerging technology of solar power system; the key areas of his presentation are topology, photonic or solar cell, power elelctronics, energy storage system and load. The design of solar power system should be smart, compact, cost-effective, reliable, robust, modular, standardized and flexible in terms of service maintenance and focused on high performance and efficiency. There are lot of scopes of improvement of the existing design of solar water heaters, pumps, lighting systems, cookers and other home

appliances in terms of appearance, size, quality, cost and product performance. The customers are very much conscious about product performance, quality of service, cost and values of a standalone solar power system. It is an interesting option to obtain system intelligence through value engineering and value analysis, brainstorming, standardization of product design, excellent quality control practice and efficient supply chain management.

Topolog*y*: One of the critical factors of system intelligence is topology of solar power system. There are different types of topologies such as standalone system, smart micro grid and hybrid system. Solar power is the modern trend of sustainable energy which requires flexible use of standalone, grid connected and hybrid system. The standalone systems are available in the form of innovative solar power enabled home appliance products such as solar cooker, lighting system, water pump, water heater and charger of computing devices. The basic components of a standalone rooftop system are solar or photovoltaic (PV) panel, inverter (optional for AC load), meter, protection relays and load. Smart Microgrids are intelligent electricity distribution networks that interconnect loads, distributed energy resources and energy storage systems within transparently defined electrical boundaries to act as a single controllable entity that can be grid connected or isolated. The system intelligence of a microgrid is associated with right sensing, communication, measurement and control technologies for effective generation and distribution of energy, self healing, stability analysis, fault analysis and load balancing mechanisms. Microgrid is an interesting and smart option of rural electrification. A hybrid system uses solar rooftop system and electrical grid alternatively according to the availability of power. There are issues of proper system integration, stability and load balancing with hybrid power system. It is logical to build an optimal number of solar thermal power plants and solar parks with medium and large capacities. But, standalone systems are also required in remote zones such as rural, forests, hilly and desert areas.

***Photonic or Solar Cell* : It is interesting to explore the dominant design of solar power system in terms of Nanotechnology based solar cells and solar power electronics. The system intelligence greatly depends on the innovation of smart materials and progress of mono and polycrystalline thin film photovoltaic technologies based on Si, semiconductors and nano PV. The efficiencies of Si and Ga As monocrystalline solar cell are relatively high. Thin film PV can reduce the cost of solar cells. CdTe and Cu (In,Ga)Se_2 thin-film solar cells have efficiencies of 21% and 20.5% respectively. The production cost of CdTe thin-film modules is about \$0.76 per peak watt; the same of mono and polycrystalline wafer Si solar is around \$1.50 per peak watt (in 2011). Silicon solar cells can be classified into crystalline and thin film cells. The maximum efficiency of a crystalline solar cell is around 25.6%; the thickness may be as high as 400 µm. Reduced reflection loss, better light trapping and improved contact area result better efficiency of crystalline solar cells. Thin film silicon solar cells have reduced thickness of 50 µm; thin films can be deposited on low cost base and the efficiency may vary between 10.5 % and 21.2% . It is required to do similar type of analysis based on real up-to-date data.**

The improved optical, chemical and electrical properties of nanomaterials can increase the efficiency of solar cells. Crystalline semiconductor III–V materials,

polymeric materials, and carbon based nanostructures are used for third generation PV cells. Third generation PVs are based on nanostructure which can improve the efficiency of solar cells at relatively low cost. Quantum wells and quantum dots are used in crystalline solar cells to achieve high efficiencies. Quantum dots are nanometer sized crystallite semiconductors. These are artificial atoms improving the energy of the carriers. Nanocrystals increase the surface area of a solar cell and absorb more solar energy. The other options are rectifying antennas using wave property of light and organic solar cells. It is really challenging to improve the efficiency of solar cells and reduce the cost of production through various strategic moves such as carrier multiplication, multi-junction cell structure, hot electron extraction, impurity and intermediate band devices. The carrier multiplication strategy increases the photocurrent generated by a solar cell and improves energy conversion efficiency by creating additional electron-hole pairs in PV devices. A multi-junction structure captures a large fraction of solar spectrum while minimizing thermal losses by stacking cells in the order of band gaps; its efficiency is 37.9%. It is essential to improve the efficiency of the solar cells through innovation of smart materials and explore economical manufacturing technology. A smart analytics needs up-to-date data on efficiency and cost of different types of solar cells.

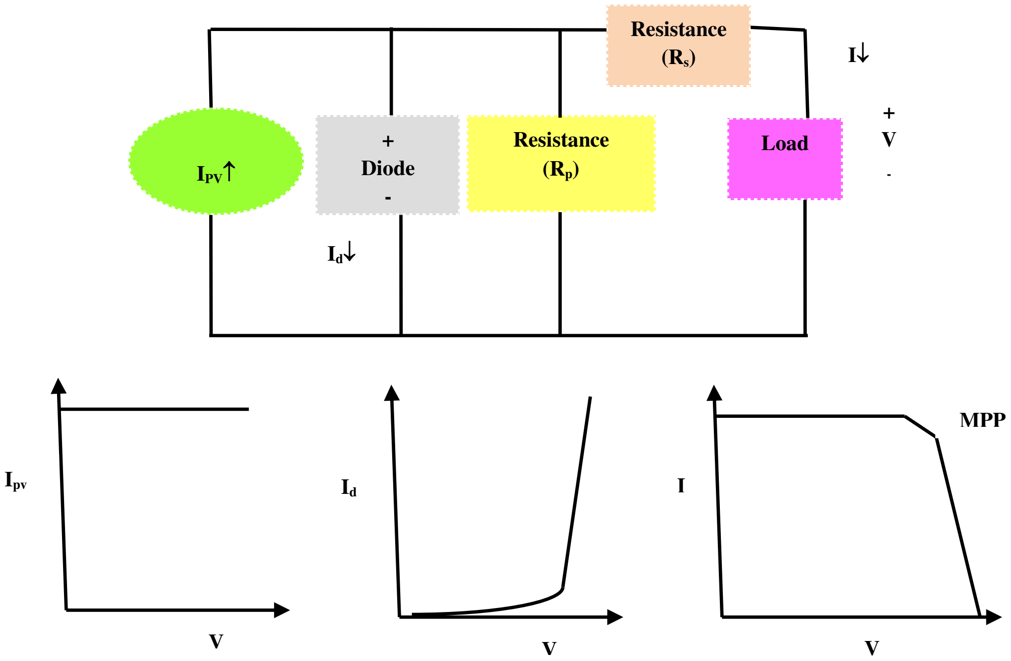


Figure 6.2 :Circuit of PV cell and Electrical Characteristics (I-V curve and MPP)

A Photovoltaic (PV) system converts sunlight into electricity directly. The basic building block of a PV system is PV cell; a set of PV cells are grouped to form panels or arrays. The cells are connected in series to obtain large output voltage. It is possible to obtain large output current by increasing the surface area of the cells or by connecting cells in parallel. A PV cell is basically a semiconductor diode with its *p–n* junction exposed to sunlight. The rate of generation of electrical carriers

depends on the flux of incident sunlight and the capacity of absorption of the semiconductor. The capacity of absorption depends on the temperature, semiconductor band gap, reflectance of cell surface, intrinsic concentration of carriers of the semiconductor, electronic mobility and recombination rate

Figure 6.2 shows the equivalent circuit of a PV cell. The basic equation describes the current (I) – voltage (V) characteristic of the ideal PV cell is $I = I_{pv} - I_0$ [exp(qV/akT) – 1] where I_{pv} - current generated by the sun light , I - Shockley diode equation; I_0 - reverse saturation or leakage current of the diode, q - electron charge (1.60217646 × 10^{-19} C), k - Boltzmann constant (1.3806503 × 10^{-23} J/K), T (in Kelvin) - temperature of the *p–n* junction and *a* - diode ideality constant. A solar panel can generate its maximum voltage in full sunlight with no load; it is open circuit voltage of the panel. As the load of the solar panel increases, the output voltage decreases nonlinearly. The power output of a PV system depends on various factors such as module temperature, dirt and dust and DC to AC conversion. The output power of a PV system reduces as the module temperature increases. Dirt and dust on the solar module surface blocks some of the sunlight and reduces output (e.g. 7%). Some power is lost through DC to AC conversion in inverters (e.g. 10-12%).

Nano technology for solar cells : The basic objective of Nanotechnology is to reduce the cost per solar cell and improve the energy conversion efficiency. The emerging technology is looking for efficient solar cells at reduced cost which can change the economics of energy market. The scope of nanotechnology may be explored in terms of nanoparticles, nanotubes, nanowhiskers as antireflective coating, multi-junction solar cells (MJSC), dye sensitized solar cells (DSSC) and quantum dot solar cells (CdSe QD). The technology of solar cells has been evolving through three generations : first generation having *crystal silicon cells* dominating the market, second generation having *amorphous silicon thin film cells* at reduced cost and third generation adopting *nanotechnology* with a mix of flexible and printable substrates and electronically conducting nanomaterials.

The structure of nanoparticles determines what range of frequencies they can resonate at or accept plasmon energy levels : roughly 575 - 9000 nm or 2.25 - 0 eV for nanoshells, 475 - 1400 nm or 2.6 - 1.0 eV and 600 -1200 nm or 2.2 - 1.25 eV for nanocubes. In dye-sensitized solar cells, electrons pass through a TiO2 layer and gather on fluorine-doped SnO2 of a glass surface. In CdSe QD system, the split and transfer process occurs between a polymer and CdSe dots, which provide tunnels to the electrodes. TiO2 only collects 5% of the solar spectrum with a bandgap of 3.2 eV. TiO2 can be doped with N. Antireflection (AR) coating and quantum wells can also improve the energy conversion efficiency. Multi-junction cell allows the absorption of larger range of wavelengths in the solar spectrum through stacking of solar cells of different band gaps in series. A 3-junction solar cell can have about 40.7% efficiency under 240-sun illumination.

Power Electronics: The next interesting issue is power electronics. Prof. Platini is trying to focus on DC-DC Boost converter, microinverter and maximum powerpont tracking algorithm.

***DC-DC Boost Converters* : A DC chopper can be used as a DC converter to step up or step down a fixed dc voltage. The chopper can also be used for switching mode**

voltage regulators and for transferring energy between two dc sources. But, harmonics are generated at the input and load side of chopper and the harmonic can be reduced by input and output filter. A chopper can operate on either fixed or variable frequency. A simple step-up boost converter is comprised of dc input voltage source V_S, boost inductor L, controlled switch S, diode D, filter capacitor C and load resistance R [Figure 6.3, 6.4] . When S is on, the current in the boost inductor increases linearly. The diode D is off at the time. When S is turned off, the energy stored in the inductor is released through diode to RC circuit. The switch is operated with a duty ratio $\delta = t_{on} / (t_{on} + t_{off}) = t_{on} / T$; T= 1/f, f : switching frequency; The average value of the output voltage is $V_O = \delta.V_S$ $.V_S.\delta.T = (V_O - V_S)(1 - \delta)T$; DC voltage transfer function $M_V = V_O/V_S = 1/ (1\text{-}\delta)$; the output voltage is always greater than the input voltage. The boundary value of inductance : $L_b = (1 - \delta)^2\delta R$; $C_{min} = \delta.V_O/(V_r R.f)$; a large filter capacitor is required to limit the output voltage ripple.

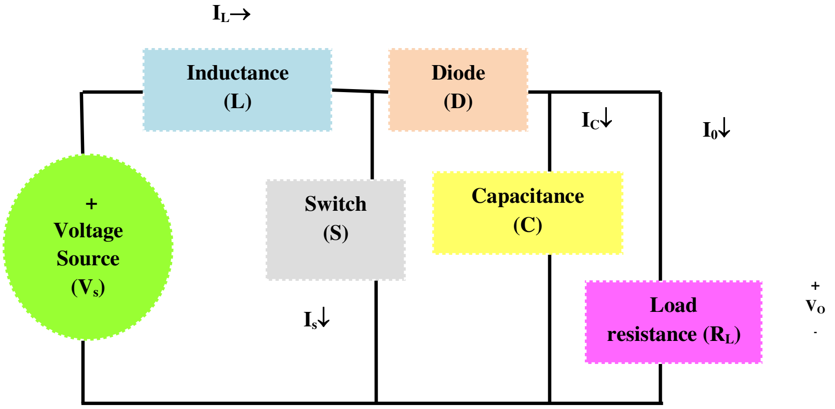


Figure 6.3 : DC boost converter – simple circuit

Let us perform the strength and weakness analysis of a DC-DC boost converter. Solar panels convert sun irradiation into electrical energy using photovoltaic effect. The output voltage of a solar panel varies based on solar irradiation and temperature; it is not possible to connect sophisticated electrical and electronic load with PV panels for this reason. So, the circuit requires a reliable and efficient DC-DC boost converter with constant step-up voltage. Here, the critical success factors are converter configuration, control mechanism, integration with power utilities, output limitation, efficiency, sensors and complex control algorithm. The cost of converter is approximately 15% of the system cost. But, there are various constraints such as reduction in gain, decreased output voltage, complex control schema, less efficiency and increased cost, variable PV power irradiation and load.

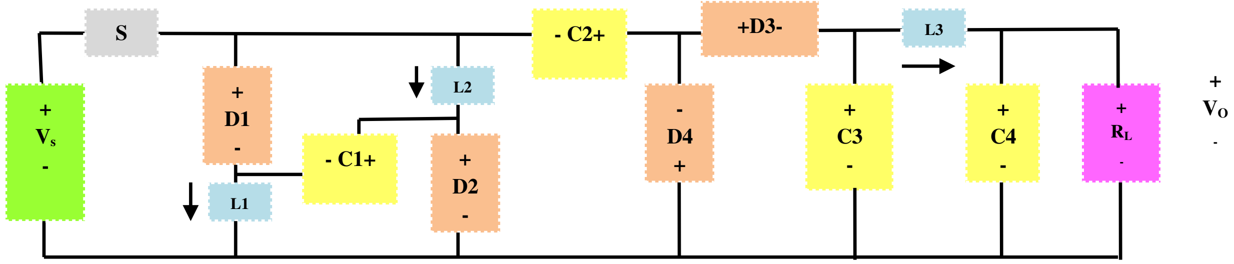


Figure 6.4 : DC-DC boost converter – complex circuit

The possible solution may be high output voltage DC-DC boost converter with MPPT algorithm based on PI controller. A PV module with parallel connection of a set of panels can obtain high current. For a PV panel, power capacity is about 100-300W, MPPT Voltage range is 15-40V, DC-DC boost converter is used for step up conversion of low voltage of a PV panel. The circuit a DC-DC boost converter consists of static switch, diodes, capacitors, inductors and load resistance. The important design parameters are input voltage, inductance, capacitance, load resistance, duty ratio, switching frequency. The other variables are supply voltage load voltage, supply current and load current.

Maximum Power Point Tracking [MPPT] **: What are the strategic options to obtain maximum available solar power from PV panels?**

- **DC-DC boost converter with high gain may be connected with an inverter;**
- **Series / parallel connection of arrays of solar panel;**
- **Maximum power point tracking algorithm (MPPT) based on PI control;**
- **The power output of solar systems increases with the use of efficient sun tracking methods such as polar axis and azimuth / elevation types. AI based solar tracking policy may consider various factors such as forecasted weather conditions, energy consumption and complex closed-loop PI control logic.**

Power Amplifier**: The system intelligence of a solar power system is highly correlated to the design and topology of power electronic circuit. The energy conversion efficiency of a photonic solar cell is low (e.g. 20%). Therefore, a solar power system needs the support of a power amplifier. It is a new concept. Let the input power of a power amplifier is p; the output of the amplifier should be P = k.p where k is a constant greater than 1. Recently, Mitsubishi Electric Corporation has developed a prototype gallium nitride high electron mobility transistor amplifier with 100W output power for satellite communications. Generally, voltage and current amplifiers are used in boost converter. A voltage amplifier can raise the voltage generated by solar panels in poor light condition.**

Is DC-DC boost converter considered as equivalent to power amplifier? What is boosted V or I? P=VI; If I ↑ and V = constant then P↑; If V ↑, I ↑; then P ↑; but increased I results overheating of electrical and electronic devices. P= Constant; if V ↑then I↓. If V↑ and I = constant then P↑; in case of PV power generation with voltage operation mode, high output voltage DC-DC boost converter maximizes the output of PV panel. Let us consider circuit intelligence of maximum power point tracking schema.

The solar power system requires the support of an intelligent load manager for effective monitoring of voltage (V), frequency (f), current (I), power (P), energy (E) and maximum power point tracking (MPPT). Maximum Power Point Tracking (MPPT) techniques find the voltage V_{MPP} or current I_{MPP} automatically at which a PV cell should operate to obtain maximum power output P_{MPP} under a given temperature and irradiance. There are different MPPT techniques such as hill climbing, Kalman filtering and perturb and observe (P&O) methods. Hill climbing

is related to a perturbation in the duty ratio of the power converter and P&O involves perturbation in the operating voltage of the solar cell. There are differences among various MPPT techniques in terms of complexity, number of sensors, convergence speed, cost, effectiveness, implementation hardware and use of soft computing based microcontrollers (e.g. Fuzzy Logic, Artificial Neural Network).

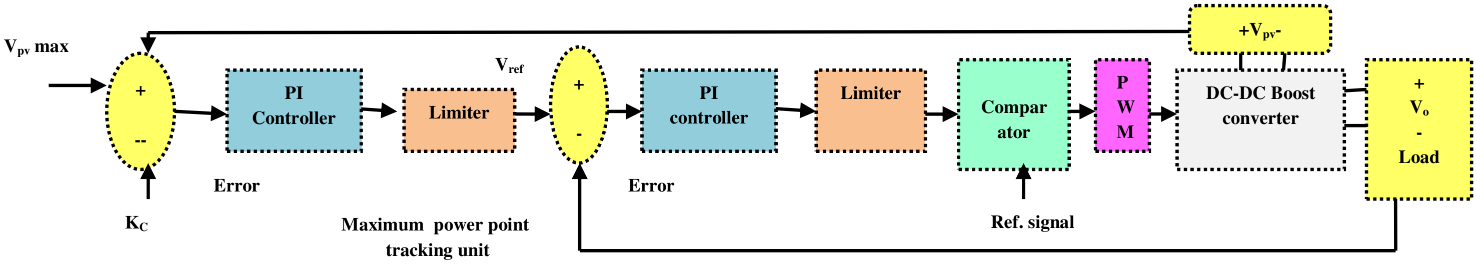


Figure 6.5 : MPPT Control Circuit

Voltage control mode is considered to maximize power generation by PV panel. For example, MPPT may be set at 10V to attain maximum power 500W. The circuit for MPPT consists of two voltage sensor feedback, two P-I controllers, two limiters and a signal compensator. The feedback voltage from PV panel is compared with maximum reference voltage and obtained error is regulated through a P-I controller to obtain the output reference voltage. It is the maximum fixed output voltage reference for the converter. The feedback from DC load voltage is compared with the reference voltage to obtain the error which is then applied to another P-I controller to compensate the error. The signal of P-I controller defines the duty ratio δ for PWM mode. δ is then compared with a ramp-signal to generate pulses for static switch of the converter circuit. The proportional and integral gain of PI controller are fine-tuned to maintain MPPT under variable irradiation and load.

Solar micro-inverter : Inverters convert from DC to AC while rectifiers convert from AC to DC. Many inverters are bi-directional; operate in both inverting and rectifying modes. A standalone PV system operates at 110/240V AC with 50/60 Hz frequency. Inverters operate at 12, 24, 48, 96, 120 or 240V. An inverter for a stand-alone PV system should have sinusoidal output voltage, voltage and frequency within allowable tolerance limits, good voltage regulation and high efficiency at light loads. Inverters use semiconductor devices such as metal oxide semiconductor field effect transistor (MOSFET) and insulated gate bipolar transistors (IGBT). These devices are used in units up to 5 KVA and 96V DC. They have the advantage of low switching losses at higher frequencies. Voltage Source Inverters (VSI) and Current Source Inverters (CSI) are usually used in standalone PV applications. They can be single phase or three phase and use square wave, quasi-square wave, and pulse width modulation techniques.

The topologies, control method (e.g. pulse width modulation [PWM], boundary conduction mode [BCM], discontinuous conduction mode [DCM]) and soft switching methodologies using MOSFETs and IGBTs are the basic elements of circuit intelligence in power electronic inverters and converters. A PV ac module is called *microinverter* which has benefits in terms of maximum power point tracking efficiency, low manufacturing cost, safe and simple installation procedure. Module integrated converters or microinverters (MICs) are designed to interface a single, low-voltage (e.g. 25–40 V) panel to the ac grid. Such converters provide benefits in terms of ease of installation, system redundancy, and increased energy capture in partially shaded conditions. An energy storage block can be used in a series connected path with the line interface block providing independent control over the capacitor voltage, soft-switching devices and full four quadrant operation with the grid. Several factors must be considered while selecting or designing an intelligent inverter for solar power system such as power conversion efficiency, electrical losses, rated power, duty rating, input voltage, voltage regulation, voltage and current protection, frequency and power factor.

A solar micro-inverter converts DC from a single solar panel to AC. The combined output from several microinverters is fed to the electrical grid. Solar panels produce DC voltage that depends on module design and lighting conditions. For example, panels using 6-inch 60 cells can produce a nominal 30 volts. The panels are connected in series to produce 300 - 600 V DC. The inverter converts this DC voltage into 110V / 230VAC, 50 Hz; microinverters are typically rated between 190 and 220 W and can tune the output of PV panel. Microinverters contrast with conventional string inverters having advantages simplicity in system design, space utilization, cooling and safety. Even small amount of shading, debris or snow lines on any one solar panel or a complete panel failure do not reduce the output of the entire array disproportionately. Each microinverter harvests optimum power through maximum power point tracking. The efficiency of a panel's output is strongly affected by the load. Inverters use MPPT to ensure optimal energy harvest by adjusting the applied load. Microinverters may not need large transformers; large electrolytic capacitors can be replaced by thin-film capacitors.

Module integrated converters or microinverters (MICs) can be used for single-phase grid-tied photovoltaic applications with a topology that places the energy storage block in a series-connected path with the line interface block. It can interface a single low voltage 25-40V PV panel to an AC grid. This design provides various types of benefits such as soft-switching for all semiconductor devices, independent control over capacitor voltage and full four-quadrant operation with the grid, ease of installation, system redundancy, and increased energy capture in partially shaded conditions. A third-port topology places energy storage buffer block in series with the line voltage interface. The topology achieves high efficiencies with its continuous constant power operation.

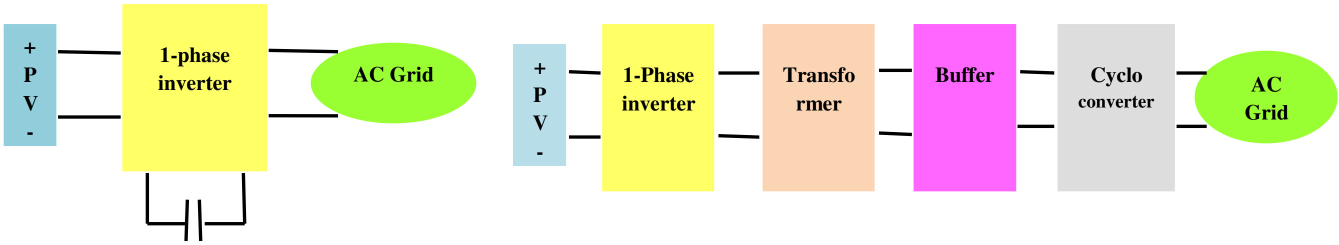


Figure 6.6 : Microinverter topology

The circuit consists of four functional blocks of the converter: (1) high-frequency resonant inverter, (2) transformation stage, (3) energy buffer and (4) cycloconverter. Each is connected in series, with a common high frequency resonant current linking them together. This topology allows bidirectional power flow in each block and it is possible to reduce heavy conduction loss through soft switching techniques. Typical rating of a microinverter is 100W,32V input, 240V output, 95% efficiency. In the classification of inverter topology, the location and the operation of energy storage buffer within the converter are two important parameters. Single stage topologies (e.g. flyback, ac-link) place capacitance in parallel with PV panel. The second option is two complete cascaded conversion stages with energy storage at an intermediate dc bus. Generally electrolytic capacitors are used for dc energy storage due to high energy density, but suffer from long-term failure rates. Photovoltaic Grid-Tied-Interleaved Flyback Microinverters can achieve high efficiency in wide load range by intelligent control strategies such as Boundary conduction mode (BCM) and discontinuous conduction mode (DCM) [Table 6.1]. In this case loss analysis plays a critical role in estimation of efficiency of flyback microinverters. The dominant losses at heavy load include conduction loss of the power MOSFETs, diodes and transformer; the dominant losses at light load include gate driving loss, turn-off loss of power MOSFETs and transformer core loss.

***Energy Storage System*: The output of solar photovoltaic system varies significantly depending on the time of a day, weather and shading conditions. The system requires a stable energy source and it should be dispatched at request. It demands an efficient energy storage system for solar power system in the form of batteries. There are different options for integrating an energy storage system into a solar PV system such as PV to grid (dc to ac), PV to battery (dc to dc), battery to grid (dc to ac), and battery/PV to grid (dc to ac). An intelligent converter can be used for both single phase and three phase PV battery application. The system is expected to have improved efficiency, reduced weight, volume and cost and minimum number of conversion stages. Li-ion battery can be used for solar energy storage system. It requires a constant current constant voltage charging algorithm. The battery should be charged at a set current level until it reaches its final voltage.**

***Load* : The system intelligence is associated with energy efficient loads and mechanisms. Energy consumption is a critical concern since energy dissipation results thermal problems in electrical and electronic devices. Energy is a critical design constraint of electrical and electronic system. There are various strategies of minimizing energy consumption in computing devices such as power down mechanisms and dynamic speed scaling in variable speed processors. The display of computing devices 9 e.g. laptops, tablets) turns off after some period of inactivity. A computing device transitions to a standby or hibernate mode if it remains idle for a while. Intelligent task scheduling can save energy consumption in micro-processor enabled devices. Today, LEDs are widely used as energy efficient lighting or illumination systems. A simple standalone solar power system is easily compatible with light load such as LED, fans, TV and energy efficient motors and computing**

devices. In agriculture, the pumps and motors should be efficient to reduce the consumption of energy. The design and selection of electrical and electronics equipments should focus on energy efficiency through intelligent algorithms and operating mechanisms.

The system intelligence depends on good design and sizing of PV cells, power conditioning system, inverters and converters, battery management system. Technology management for solar power electronics requires discriminatory, fair and rational pricing mechanisms, incentive and subsidy policy, economies of scale of mass production, strategic cost reduction, product life-cycle management, quality policy and intelligent cost-benefit analysis. Solar power electronics face two critical constraints which should be improved through innovation, strategic alliance and intelligent technology management in future : high cost of production and low efficiency in conversion of sun light into electrical energy. It is essential to explore intelligent business models and applications of solar power such as rural electrification, agriculture and solar cooker. It can be a blue ocean space in energy business.

4. SECURITY

Security Analytics

Security schema :

- **Snubber circuit for high dv/dt and di/dt protection**
- **Fuses for fault protection**
- **Heat sink for thermal runaway**
- **Reverse recovery transients**
- **Supply and load side transients**

Emerging technologies:

- **Digital relays for voltage, current and frequency protection;**
- **Earthing system: Earthing rod, lightning arrester;**
- **Switchgear : Fuse, MCB, Circuit breaker;**
- **Load manager for maximum power point tracking;**

***Verification mechanism*: audit *security intelligence* of solar power technology.**

- ***system performance:*** **verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness, reachability, synchronization, safety;**
- ***multi-party corruption*** **in case of quality problem;**
- ***access control in R&D*: verify authentication, authorization, correct identification, privacy, audit confidentiality, data integrity and non-repudiation;**
- **System design: verify rationality, fairness, correctness, transparency, accountability, trust and commitment;**
- ***malicious attacks*: false data injection, shilling: push and pull, denial of service (DoS), fault injection attack;**

call threat analytics and assess risks of emerging solar technology :

- **what is corrupted or compromised (agents, technology schema)?.**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**

- **insights : how and why did it occur? do cause-effect analysis on performance, sensitivity, trends, exception and alerts.**
- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**

***Output*: security intelligence**

Prof. Bruno Platini is also presenting the security of solar power system : how to verify the security intelligence of solar power system? It is essential to verify security intelligence of this technological innovation collectively through rational threat analytics at five levels: L1, L2, L3, L4 and L5. The basic building block is an intelligent threat analytics. At level L1, it is required to verify the efficiency of access control in terms of authentication, authorization, correct identification and audit Only asset of authorized entities or agents are able to access the technology of solar power system through authenticated channels. The technical specifications od solar power system and the demand of the clients and consumers should be correctly identified bu the service providers and producers. At level L2, it is essential to evaluate rationality fairness, correctness and transparency of solar power technology management strategy through SWOT analysis, TLC analysis and also technology innovation, adoption and diffusion strategy, At level L3, it is rational to assess the risk of various types of malicious attacks on solar power technology such as fault attack, Denial of Service (DoS), Sybil, false data injection and shilling attacks. The adversaries may execute push and pull attack by other existing power generation and distribution technologies by adopting irrational, incorrect and biased analysis for technology diffusion strategy. An adversary is a malicious agent who attacks solar power system and the associated protocols; the basic objectives are to cause disruption and malfunctioning of a secure system. The security element should be analyzed in terms of the assumptions, goals and capabilities of the adversary. It is also crucial to analyze the adversary model in terms of environment, location, network, resources, access privileges, equipments, devices, actions, results, risks, reasons and motivations of attacks and probable targets. At level L4, it is required to assess the threats of multi-party corruptions on solar power system. The corrupted entities may be trading agents, producers of solar cells and panels, service providers, system administrators and support staff.

Finally, at level L5, it is crucial to audit the solar power system performance in terms of in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety. The performance of solar power system and quality of service is expected to be consistent and reliable. Safety indicates that under certain conditions, an event (e.g. electrical faults like overcurrent, overvoltage, short circuit, earth fault, under voltage, over frequency, under frequency) never occurs. Safety is a critical requirement of solar power system system whether it is mechanical, electrical, electronics, information technology, civil or instrumentation engineering. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of solar power system. Another important issue is robustness of a

system. The delivery of the output should be guaranteed and the adversary should not be able to threaten a denial of service attack.

Another important issue is the protection of power electronic circuit used in solar power system. The threat analytics analyzes the power electronics circuit from five different perspectives: snubber circuit for high dv/dt and di/dt protection, fuses for fault protection, thermal runaway by heat sinks, reverse recovery transients, supply and load side transients. Voltage transients are caused in converter circuit due to reverse recovery process of power electronic devices and switching actions in the presence of circuit inductance. Short circuit faults may result excessive current flow in power electronic circuit.. Overheating may occur due to losses in semiconductor devices; it must be dissipated sufficiently and effectively for operating the device within upper temperature limit otherwise it may affect the reliability and consistency of power electronic circuit. Fuses are used for overcurrent protection. Power converters may develop short circuit or faults and the resultant fault currents must be cleared quickly. Fast acting fuses are normally used to protect semiconductor devices. As the fault current increases, the fuse opens and clears the fault current in few milliseconds. It is essential to select the location of fuse in the power electronic circuit; generally a fuse is connected in series with each device. A fuse is selected based on the estimation of fault current. A fuse must carry continuously the device rated current; it must be able to withstand voltage after arc extinction; peak arc voltage must be less than peak voltage rating of the device.

Next, let us consider cooling by heat sink. Heat is generated due to on state and switching losses in power electronic devices. The heat must be transferred from the power electronic devices to a cooling medium to maintain junction temperature within specified range. Convection cooling is commonly used in industrial applications. It is rational to consider a set of important design parameters of heat sink such as contact area between device and heat sink, correct mounting pressure of the device on the heat sink, material (e.g. Al), size, and thermal resistance of power devices. Let us consider a power electronic circuit where a voltage source is connected in series with three resistances. $T_j = P_a(R_{jc}+ R_{cs}+R_{sa})$; T_j : junction temperature, P_a :average power loss, R_{jc} : resistance from junction to case; R_{cs} : thermal resistance from case to sink, R_{sa} : resistance from sink to ambient; T_a : Ambient temperature

It is alos essential to consider the protection through snubber circuit. It limits di/dt and dv/dt; since transients may occur in power electronic circuit. $di/dt = I_L/t_r = I_{Cs}/t_r$; during turn on collector current rises. $dv/dt = V_s / t_f = V_{cc}/t_f$, during turn off, collector emitter voltage must rise in relation to the fall of I_c. Snubber circuit protects the power electronic circuit within allowable limit of di/dt and dv/dt. Inductor L_s limits di/dt; it is a series snubber. RC snubber is normally connected across a semi-conductor device to limit dv/dt within maximum allowable rating. There are three types of snubber circuit : polarized (Resistance R limits forward dv/dt); reverse polarized (Resistance limits discharge current of the capacitor) and unpolarized (semiconductor devices are connected in parallel).

Finally, we consider the risk of transients. There are three types of transients - reverse recovery transients, supply side transients and load side transients. In case of supply side transients, a transformer is normally connected to the input side of

converters. Under steady state conditions, an amount of energy is stored in the magnetizing inductance L_m of transformer and switching off the supply produces a transient voltage at the input of the converter. A capacitance C is connected across the secondary of a transformer to limit transient voltage and a resistance is connected in series with C to limit transient voltage oscillation. In case of load side transient voltage, under normal condition, an amount of energy is stored in the supply and leakage inductance of the transformers. When the load is disconnected, transient voltages are produced due to the energy stored in the inductance. In case of reverse recovery transients,

In a circuit, voltage source Vs is connected with an inductance L, capacitance C and resistance R and a diode D_m is connected across C and R. Due to reverse recovery time t_r and recovery current I_r, an amount of energy is trapped in the circuit inductance and transient voltage appears across inductance. In addition to dv/dt protection, snubber circuit limits peak transient voltage across inductance. The snubber also limits peak transient voltage across device. The values of snubber circuit R and C are selected so that the circuit is slightly underdamped. The peak reverse voltage depends on damping ratio and current. The energy stored in inductance L is transferred to the snubber capacitance C and is mostly dissipated in snubber resistance. $L.di/dt + R.i + (1/C). \int i\, dt + v_c(t=0) = V_s$;$V= V_s - L.di/dt$; $i(t=0) =I$; $v_c(t=0)=0$

The intelligence in selection of protective system and load monitoring depends on the complexity of system topology, scalability of operation and cost. A standalone solar power system may be protected by a digital relay having features of over voltage, over current, over frequency, under voltage, under frequency, earth fault and short circuit protection. Additionally, the system should be equipped with switchgear devices like fuse, miniature circuit breaker (MCB), earthling system and simple switches. The power electronic circuit should be protected appropriately. Less harmonic should be injected by inverters to avoid heating, thermal losses and damage of consumer electronics and home appliances. Photovoltaic inverters must be able to withstand overloading for short term to take care of higher starting currents from pumps and refrigerators. The other protection issues are related to over/under voltage and frequency, short circuit, surge protection, low idling and no load losses, low battery voltage disconnect and low audio and radio frequency noise. A solar park should be protected by heavy duty equipments such as air circuit breakers (CB), MCCBs, isolators, lightning arresters (LA), power control panels and sophisticated digital relays. The cost of the protection system and load manager is a function of scalability of operation and complexity of the system configuration.

Prevention and detection are traditional approaches to the security of power system. In the context of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security but should adopt adaptive security through intelligent analytics. Advanced analytics is the basic building block of next generation security protection of solar power system which should be able to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns

by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture. Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjusts individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size complexity of solar power system – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging solar power technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures.

Solar power system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of the solar power system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. Let us explain the objectives of adaptive security in depth. New threats are getting originated as an outcome of solar technology innovation and may cause new forms of disruptions with severe impact. The system demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

5. STRUCTURE

Structure Analytics

***Agents*: system analysts, business analysts;**

***Moves*: Design and configure**

- **Solar power system architecture**
    - **Smart microgrid**
        - **AC Coupled microgrid**
        - **DC couple microgrid**

        - AC-DC coupled hybrid microgrids
    - AC / DC Sources and loads
    - Renewable energy system
    - Energy storage system
- Organization structure
    - Technology forums
    - National level : Government (E-governance model), research organizations;
    - International level : strategic alliance among global organizations

Dr. Paolo Maradona is discussing the structure of solar power system in terms of smart microgrid, various topologies such as AC coupled, DC coupled and ACDC coupled hybrid microgrids, AC/ DC sources and loads, renewable energy system (e.g. PV or solar power system), capacity and access oriented energy storage system, stand alone and grid connected operation mode, power management strategies and control schemes for both steady state and transient conditions [refer: appendix].

Smart grids are considered as next generation power systems which interconnect a set of microgrids consisting of Distributed generations (DGs) and renewable energy (RE) resources (e.g. solar, wind, tidel, clean alternative energy sources. Hybrid AC/DC microgrid contains both AC/DC power sources and AC/DC loads. It can be classified into three categories based on how the sources and loads are connected to the system and how AC and DC buses are configured into low and high frequency AC-coupled, DC-coupled and AC-DC-coupled microgrids [38-43]. In AC-coupled hybrid microgrids, DGs and SEs are connected to the common AC bus through their interfacing converters. In DC-coupled hybrid microgrids, DGs and SEs are connected to the common DC bus and an Interfacing Converter (IFC) links DC and AC buses. In AC-DC-coupled hybrid microgrids, DGs and SEs are connected to DC and AC buses and the buses are linked by Interlinking Converter (ILC). The basic objective of energy management is to match demand and supply of power optimizing cost (e.g. fuel, capital and maintenance costs), voltage and frequency regulations and real-time power dispatching among different power sources in micrograms. Microgrid architectures can be classified utility, industrial, commercial and remote type based on applications. In the appendix, table 7.1 compares various structures of microgrids based on a set of evaluation parameters such as topology, structural complexity, operation mode, control schema, power management strategies, cost and benefits.

Hybrid DC- and AC-Coupled microgrids integrate a variety of DER units into existing distribution system. It connects the distributed energy storage systems like batteries and fuel cells to bidirectional AC-DC converters and PV systems connected through DC-DC Boost converters. Microgrids can be classified into single and two stages power conversion systems [Appendix: Figure 6.12]. In single-Stage power conversion systems, a transformer is used for isolation or voltage conversion . It is a very simple structure having high efficiency, small size and weight and reduced cost. Two-Stage Power Conversion is the most common configuration for all electronically coupled DER units and it consists of a DC-DC converter for energy sources with DC output voltage or an AC-DC converter for energy sources with AC

output voltage with a grid-connected DC-AC converter. The converter on the energy source side extract the maximum power from the primary energy source and the grid side converter is controlled to follow grid requirements. Multilevel converter reduces the cost and improves the efficiency of power conversion systems. A power electronics enabled microgrid consists of a static transfer switch (STS), distributed critical and noncritical loads, multiple DER units with various power electronics interfaces, protection devices and measurement, monitoring, and control units. DC microgrids are used in telecommunication systems, electric vehicles office buildings, commercial facilities, Photovoltaic (PV) and fuel cell system. HFAC Microgrids are generally used in distributed power systems for military and aircraft systems working in single-phase 400 Hz. It is an interesting agenda to explore the use of solar power for DC microgrids application.

Microgrid is the basic building block of the future flexible, reliable and smart power grid with increased penetration of Distributed Energy Resources (DER) such as solar or PV panels. The entire architecture of future electrical power system may consider three possible concept models : Microgrids, ICT driven Active Networks and Internet. Microgrid paradigm interconnects multiple customers to multiple DER units including DG and Distributed Storage (DS) units and form an intentional or non-intentional energetic island in the electrical distribution network. The customers and DER units can operate in parallel with the main grid and supports a smooth transition during abnormal grid conditions. The evolution and rapid development of efficient power electronics technology improves the transient response, Digital Signal Processors (DSP) reduce the processing time and support complex control algorithms and efficient power electronic converters enable cost-effective and flexible control, power management and energy flows efficiently. This structural analysis is the basis of the vision of an efficient solar microgrid or solar park for rural electrification and agricultural application.

6. STRATEGY

Strategy Analytics

***Agents*: System analysts, business analysts, technology management consultants;**
***Strategic moves* :**

- **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements – scope, system, structure, security, strategy, staff-resources, skill-style-support;**
- **Define a set of energy security goals and emerging technologies accordingly.**
- **Do SWOT analysis: strength, weakness, opportunities and threats of existing technologies related to energy security.**
- **Fair and rational business model innovation associated with solar power**
  - **Who are the consumers?**
  - **What should be the offering of products and services?**
  - **What do the consumers value?**
  - **What is the rational revenue stream?**
  - **How to deliver values to the consumers at rational cost?**

- **Do technology life-cycle analysis on 'S' curve : presently at emergence phase of 'S' curve.**
- **Explore technology innovation-adoption-diffusion strategy for solar power system.**
- **Explore innovation model and dominant design of solar power system.**
- **Adopt '4E' approach for the development of underdeveloped zone by building smart villages and optimal resource planning, allocation and distribution : Envision, Explore, Exercise, and Extend.**

Prof. Johan Macacini is exploring the strategy for the innovation, adoption and diffusion of solar power technology. This element can be analyzed from different dimensions such as SWOT analysis, technology life-cycle analysis, R&D policy, learning curve, shared vision, communication protocol and knowledge management strategy.

SWOT Analysis : **The technology of solar power is related to the problem of energy security. The people in today's world are faced with significant challenges in energy sector such as shortage of energy, high cost of power generation and distribution, power distribution loss, environmental pollution, greenhouse gas emission and rural electrification. We must set an efficient national and global energy policy to promote the development of a sustainable energy system which should be viable environmentally, socially and economically based on solar power. The sustainability in energy not only requires the development of renewable energy but also promotes the use of energy efficient system such as LED lighting system which slows down the growth of energy demand and promotes the concept of clean energy that can cut down the usage of fossil fuel significantly.**

Let us first do the SWOT analysis on solar power. Renewable energy uses natural energy sources such as sun, wind, water, earth's heat and plants. There are different types of renewable energy such as solar, wind, hydropower, ocean or tidal, geothermal and bio-energy. Clean and green renewable energy technologies turn these fuels into electricity, mechanical, heat and chemical energy. It is basically an initiative of natural resource planning (NRP), a specific case of ERP. The world has limited supply of fossil fuels; there are critical issues of environmental pollution, safety and problem of waste disposal, rapid growth of energy demand. The use of thermal and nuclear power cause global warming which in turn results increase in sea level, flood, drought, heat wave and different types of natural disaster. Air pollution is one of the most dangerous killers worldwide – more than alcohol, sugar and kidney failure. The main cause of air pollution is the burning of fossil fuels. The crisis of global warming is associated with rising seas, catastrophic flood, devastating heat waves, changing heat structure of the atmosphere, unprecedented hurricanes, summer storms and smog. These events clearly show how the traditional old power plant engineering technologies are affecting the climate and weather globally. Renewable energy is plentiful and the technologies are improving rapidly. Solar technologies convert the infinite power of the sun into heat, light and power. Solar electricity or photovoltaic (PV) technology converts sunlight directly into electrical energy. Solar energy is a potential option for sustainable global energy demand. The PV market is growing rapidly.

National energy policy should be redefined since solar energy is an alternative source of energy and a substitute of traditional sources of energy such as thermal, hydel and nuclear power. It is essential to define a clear vision on renewable sources of clean energy such as solar power and set up relevant advanced research institutes to ensure energy security. Sufficient capital has been already invested on thermal, diesel and hydel power. The initial investment on hydel power plant is very high. It is not a good option for hot and dry zone where there is scarcity of water (e.g. drought in Brazil). The tribal workforce should be relieved from hard mining career (e.g. coal) in future. The nuclear power is very expensive due to shortage of fuel (e.g. Uranium). The coastal zones need several solar and wind power plants; it may be a hybrid system. Land may not be a constraint for the adoption of solar power; there is large barren land in rural zone; coastal areas, desert, hills, plateau and forests. The barren land may be utilized for solar park. It is possible to adopt 'million roof program with solar power'. It is possible to make strategic alliance with reputed solar energy vendors and manufacturers of Germany, Japan, USA, China and Israel for fast and efficient implementation of solar power system. It is possible to build many solar parks but it is also required to promote intelligent standalone solar power system. This change in energy policy is not a simple, trivial problem. The people expect more dynamic and active performance from Solar Energy Society and Rural Electrification Corporation Limited. It is required to define an intelligent solar energy policy, imports of PV modules and anti-dumping strategy.

The strong points of solar power are direct conversion of solar radiation into electricity, no mechanical moving parts, no noise, no high temperatures, no pollution. PV modules have a very long life-time, the energy source i.e. the sun is free, ubiquitous, and inexhaustible. PV is a very flexible energy source, its power ranges from microwatts to megawatts. Solar power can boost the growth of various types of industries like photovoltaic cells or modules, power electronics devices (e.g. power amplifiers, converters and inverters), battery and energy storage devices, intelligent load managers with power tracking capabilities, smart micro-grid, steel and aluminum structures. It can reduce the cost of power generation, transmission and distribution and power distribution loss significantly. But, there are few constraints of this technology such as low efficiency of solar cell, maintenance, cleaning of dust, dirt and moisture from solar panels and the negative impact of natural disasters like storm, rainfall and snowfall.

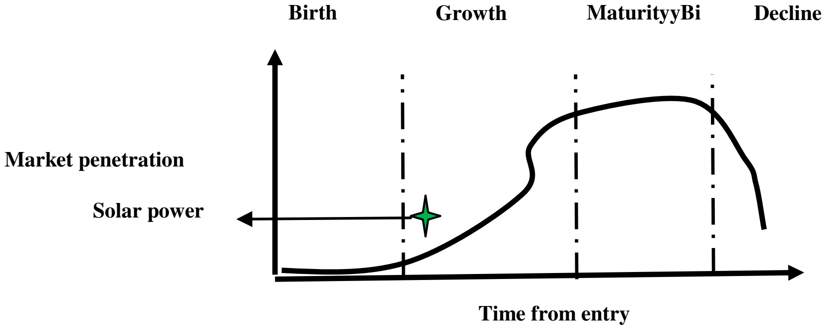


Figure 6.7 : Technology life–cycle analysis

Technology Life-cycle Analysis : **Deep analytics evaluates and explores top technological innovations in terms of technology life cycle, technology trajectory, S-curve, technology diffusion and dominant design. Technology trajectory is the path that the solar technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors on solar technology trajectory today. How to manage the evolution of this technological innovation? The nature of innovation may shift after a dominant design emerges. At present, the solar technology is waiting for the dominant design. The diffusion indicates how new solar technologies will spread through a population of potential adopters. It is controlled by the characteristics of innovation, economic environment and the adopters like innovators, early adopters, early majority, late majority and laggards.**

At present, the technology of solar power is at growth phase of technology life-cycle [Figure 6.7]. It has come out from the emergence phase. It is interesting to understand how the life-cycle of solar technology is interacting with other technologies, systems, social impact, life-style and culture. The solar technology has been evolving from its parents such as other branches of electrical power system and electronics engineering; they are interacting with each other to form complex technological ecologies. The parents are adding their technological DNA which are the basic building blocks of new product development. A new development of solar technology must be nurtured properly since many technologies had perished at the emergence phase due to inherent constraints, uncertainties and risks. Next phase is growth; the solar technology has survived its early phases, it is adapting to various challenges of business model innovations and is forwarding to its intended environment with the emergence of competitors. It is basically the question of struggle for existence and survival for the fittest of the dominant design.

Initially, it may be difficult and costly to improve the performance of new solar technology; it may be costly for the adopters due to various uncertainties and risks. The performance is expected to improve with better understanding of the fundamental principles and system architecture. Gradually, this new technology may be adopted by large segments of the market due to reduced cost and risks. The rate of improvement of the new solar technology may be faster than the rate of market demand over time; the market share is expected to increase with high performance. The evolution of the solar technology is now passing through a phase of turbulence and uncertainty; various stakeholders of the supply chain are exploring different competing design options and a dominant design is expected to emerge in near future through the consensus and convergence of the system intelligence. Then, the producers will try to improve the efficiency and design of solar power systems based on stable benchmark of the industry. The dominant design must consider an optimal set of most advanced technological features which can meet the demand of the users, supply chain and design chain in the best possible way.

***Quantitative Analysis*: It is essential to exercise intelligent quantitative analysis through business analytics and technical analytics based on up-to-date technical and business data. Both types of analytics are closely associated. The scope of business analytics should be explored in terms of installed power generation capacity: Energy type, capacity (MW/GW), Period (year); PV market analysis based evolution of PV modules production : The basic parameters for this analysis may be energy sources (e.g. solar, wind, tidel, thermal, hydel, nuclear), market share, zone and growth rate; SWOT analysis; Period (year), zone, PV production; Top PV cell production companies, Period (year), MW; Type of PV cell, MW and PV Module comparison based on efficiency, and power rating.**

The scope of technical analytics should be explored through advanced experimental set up and graphical data visualization techniques.

- **Solar cell**
    - **Cost vs. efficiency analysis : solar cell type (e.g. 1st, 2nd, 3rd generation), material (Si, III-V, II-VI, I, III, VI, Nano PV), , cost , energy conversion efficiency;**
    - **V-I characteristics : short circuit, open circuit, MPP at different irradiation and temperature**
    - **P-V characteristics for equivalent series and parallel resistance**
    - **Absolute error vs. voltage**
    - **Company, device, size, efficiency (%), Power (MW);**
    - **PV cell material, optimal absorption, band gap (minimum and maximum eV);**
    - **Deposition time vs. evaporation rate**
- **Power electronic circuit performance analysis:**
    - **DC-DC boost converter**
        - **Performance analysis: input voltage, input current, input power, output voltage, output current, output power, duty ratio, efficiency (%), ripple (%)**
        - **Transient performance analysis : time (S) vs. output voltage (V), time (S) vs. output current (A) under varying load and irradiation;**
        - **Converter type (classical, proposed), output voltage, output current;**
        - **Simulation testing analysis : input voltage, inductance, capacitance, load resistance, duty ratio, switching frequency;**
        - **MPPT analysis : PV panel rating, rated voltage, rated current, rated power, open circuit voltage, short circuit voltage, short circuit current, MPPT;**
        - **Duty ratio vs. output voltage graph;**
        - **3-D Radar plot of performance measurement: output voltage (V), output current (A) and efficiency (%);**
        - **PV panel output analysis : voltage (V) vs. current (A), voltage (V) vs. power (W);**
    - **Photovoltaic module integrated Inverter or micro-inverter**
        - **Performance comparison of various types of micro-inverters : topology (series buffer, parallel buffer, flyback, boost, AC Link),**

    - **energy storage, input voltage (V), rated power(W), efficiency, reactive power, complexity (low, medium, high);**
    - **Input voltage, output voltage, output power, line frequency;**
    - **Switching frequency, buffer voltage, inductance, capacitance, transformer turns ration, MOSFET rating, resonant inductance and capacitance;**
    - **Waveform analysis : current, voltage, line phase vs. current, line phase vs. phase shift, line voltage phase angle vs. impedance, line phase vs. efficiency; current waveform of flyback inverter under BCM and DCM control, input and output waveform, PV voltage vs. PV current, PV voltage vs. PV power, PV voltage and current under half and full load conditions, grid voltage and current under half and full load conditions;**
    - **Comparative analysis on BCM and DCM in terms of switching frequency, power transfer, peak current sensing, loss analysis under high and low load, efficiency vs. output power**
- **Battery performance analysis in terms of battery capacity, nominal voltage, minimum battery voltage, maximum discharge current, maximum charging voltage, maximum charging current, steady state and transient analysis;**
- **Temperature profile of solar cooker (Time vs. Temperature)**

Shared vision **: Efficient change management is one of the most critical success factors in solar system implementation. It ensures that an organization and its workforce are ready, willing and able to embrace the new business processes and systems. The change management is a complex process. The change should occur at various levels: system, process, people and organization. Communication is the oil that ensures that everything works properly in solar system implementation. Management's honest determination to exert and maintain its right to decide within a policy of fairness and openness is essential for successful change management. An efficient leader creates understanding among his workforce through intelligent corporate communication.**

Communication protocol **: It is essential to communicate the scope of solar power to the common people, corporate sector, public policy makers, state and central governments, academic and research community through popular broadcast communication channels (e.g. TV, radio, social media, social networking sites, SMS, MMS, corporate web portals etc.) and adoption of rational and intelligent programmes, advertising and promotions. It is also possible to make innovative and creative documentary films on solar power evolution and broadcast the same to the academic and research community through school and college education systems and YouTube channels. It is rational to focus on introduction of courses on renewable energy and solar power in academic programmes of Electrical and Electronics Engineering (e.g. B.Tech, M.Tech, B.E.E, M.E., Ph.D.) and also business management (e.g. Technology Management, Strategic Management and Business Analytics for BBA, MBA, PGDM, PGDBM).**

Goal : **The strategic intelligence is associated with good governance, good wishes in public policy, industry analysis, efficient enterprise resource planning, supply chain management and marketing efforts (e.g. pricing, promotion, trust in communication, sales and distribution). Let us first consider *pricing strategy*. The diffusion of solar power requires a rational, discriminatory and fair pricing mechanism, incentive and subsidy policies. Industrial power play may be a serious threat against the adoption of solar energy. Existing power generation, transmission and distribution companies are comfortable with traditional thermal power technology. The coal, oil and gas industries are also not comfortable with the emerging trends of renewable sustainable energy. They do not want to save precious fossil fuels and oil. That is why, the old power generation and distribution firms are not serious in R&D and deployment of solar power system globally. Solar power is a real transformation initiative and the old firms are trying to resist against this change. Our society needs fundamental rethinking and radical redesign of energy policy. The pricing policy of solar power system (e.g. energy service charge, price of standalone solar power systems) should have necessary *competitive intelligence* to conquer the aforesaid threats.**

Next, let us consider the *promotional strategy*. An intelligent marketing strategy is essential for proper technology management and enhancement of the awareness of new solar technology. The trade fairs and energy summits are expected to perform live product demonstration and interactive brainstorming sessions; audio and video display of solar power plants and standalone systems already in use in various places of the world; invite national and international technical experts and scientists from industry and academic institutions; invite energy policy makers, consultants, engineers, students, strategists, architects, construction and infrastructure project managers, entrepreneurs, traders, venture capitalists, banking & financial institutions (e.g. rural banks, national banks); invite Business Intelligence analysts to discuss possible growth roadmap and publish smart product catalogues and brochures. Event management plays an important promotional strategy; various workshops, conferences and seminars should encourage exchange of innovative ideas among the experts. There are other important initiatives such as training sessions for the workforce of construction and infrastructure firms, power generation, transmission and distribution companies and contractors; advertisements in popular business and industry magazines and daily newspapers; intelligent broadcast through TV, radio and corporate communication channels; pilot projects in villages, hilly areas, forests and deserts and active involvement of gram panchayat and municipal corporations in solar power system implementation programmes.

Another critical strategy is related to *production process and supply chain management of solar cells*. Sustainable photovoltaics need the production of next-generation smart materials, devices and manufacturing processes suitable for global needs, environment and resource availability, advanced manufacturing process and multi-scale modeling and reliability. Solar energy integration is a critical issue; it is essential to identify and assess key technical, economic, environmental, and policy barriers in the adoption of solar power globally. For correct road mapping and assessment, it is required to analyze market research, policy and technical data,

solar energy integration, storage and multi-scale (10 - 500 kW) concentrating solar power systems.

Dominant design : **The technology of solar power is going through an evolution. The emerging technology is trying to achieve a *dominant design* which may have two major aspects: (1) solar power electronics resulting an intelligent circuit and (2) Nanotechnology based solar cell as stated above. Dominant design is a concept of technology management, identifies key technological features that become a de facto standard. The innovators must try to explore dominant design to win the market share. The dominant design may be a new technology, product or a set of key features as the outcome of a set of independent technological innovations. When a new technology emerges, different firms introduce a number of alternative designs based on incremental improvements. The dominant design enforces standardization, results economies of scale and competition starts based on cost, scale, product features and performance. Dominant design may not be better than other designs; simply incorporates a set of key features that emerge due to technological path-dependence and not necessarily stricts customer preferences. Dominant designs are expected to acquire more than 50% of the market share. The process of dominance passes through a few milestones. An innovator conducts R&D to create a new product or service or improve an existing design. The first working prototype of emerging technology may send a signal to competitors to review the feasibility of their research programs. The first commercial product is launched and directed at a small group of customers and force the competitors to review and speed up their research efforts. A clear front runner emerges from the early market. Finally, a particular technological trajectory achieves dominance.**

Technology trajectory **is the path that a technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors and patterns of technology trajectories of solar power system today. How to manage evolution of technological innovation? The nature of innovation shifts markedly after the dominant design emerges. The pace of performance improvement utilizing a particular technological approach is expected to follow S-curve pattern. The evolution of innovation is determined by intersecting trajectories of performance demanded in the market vs. performance supplied by solar cell technology. Technology diffusion of solar power indicates how new technologies spread through a population of potential adopters. It is controlled by characteristics of innovation, characteristics of social environment and characteristics of the adopters such as innovators, early adopters, early majority, late majority and laggards. From the perspective of solar power, the basic objectives of technology management include several issues such as integrated strategic planning, forecasting, design, optimization, operation and control of products, processes and services to understand the dynamics of technology innovation, hype, priority, capability, maturity, adoption, diffusion, infusion, transfer, life-cycle, dominant design, spillover effects, blind spots and also the value of this emerging technology for our society. The basic objective of technology forecasting is to predict the future characteristics of solar power system.**

Let us consider the issue of solar technology innovation, adoption and diffusion. We should analyze how over time an idea or product associated with solar power gains momentum and diffuses or spreads through a specific population or social system. Diffusion is the process by which innovations spread in our society over time, adoption is a decision of implementing innovations based on knowledge, and persuasion of individuals within a given system. The diffusion of innovation is the process by which new products are adopted by their intended audiences. It allows designers and marketers to examine why it is that some inferior products are successful when some superior products are not. Diffusion of innovation is responsible for the launch and spread of some of the most important advanced solar technologies in human society globally,

Technology diffusion **is the process by which innovations of emerging solar technology is adopted by a population. The rate of diffusion depends on several factors such as nature and quality of innovation, how information about the innovation is communicated and characteristics of the population into which the technology is introduced. Why is technology diffusion important? Technology diffusion plays a major role globally today. We can increase the trade by removing the diffusion barriers since the countries achieve higher productivity by taking the technology from the diffusion process. What is meant by technology diffusion of solar technology? Technological diffusion is the process by which innovations (new products, new processes or new methods) spread within and across economies. What are the steps of diffusion? Diffusion occurs through a five step decision making process. It occurs through a series of communication channels over a period of time among the members of a similar social system. The five stages are awareness, interest, evaluation, trial, and adoption of solar technologies. The goal of this diffusion strategy is to spread the word about the innovation and encourage users to adopt it. These strategies may also be modified and used to target any other user group. The rate of diffusion is the speed with which the new idea spreads from one consumer to the next. Solar technologies have been evolving from various interesting applications; the rate of diffusion depends on the support of government's energy security policy globally.**

Let us consider solar *technology spillover effects*. Technology spillover is ultimately a learning experience. A group of firms from emerging economies may enjoy unintentional technological benefits from R&D efforts of leading firms of solar technology from advanced economies (without any additional cost sharing. Successful technology spillovers depend on the absorptive capability of the receiving firms, technological gaps, interactions, information symmetry, strategic alliance, joint venture and knowledge flows between sending and receiving firms and also geographical and cultural proximity of a social process. Technology absorption is the acquisition, development, assimilation and utilization of technological knowledge and capability by a firm from an external source; it occurs between transferring and receiving entities. What factors influence the rate of adoption and diffusion of solar technology innovation? There are specific product and service attributes that affect the diffusion process and can influence consumer acceptance of new products and services; these factors are relative advantage, compatibility, complexity, trialability and observability. Transfer of technology is

the process of transferring or disseminating technology from one country that owns or holds it to another country through strategic alliance and joint ventures, Solar power system has been becoming more intelligent, advanced and efficient. Solar technology has a great positive impact on our life. New technology always changes our life very much and takes it to a new level. It is like the new ways of thinking or doing the normal things differently, better with less hassle and at a much affordable rate.

Another important issue is *technology adoption* of solar technology. Within the rate of adoption, there is a point at which an innovation reaches critical mass. The categories of adopters are innovators, early adopters, early majority, late majority, and laggards. Diffusion is a macro process concerned with the spread of a new product from its source to the consuming public. Solar technology diffusion is a measure of how widely technology is spread globally from the developed countries to the developing and undeveloped countries. Adoption is a micro process that focuses on the stages through which an individual consumer passes when deciding to accept or reject a new product. There may be various strategies of solar technology adoption : align technology and strategy; communicate for buy-in and engagement; perform a current systems analysis; develop training approach early and integrate technology deployment with change management and create an effective governance structure for solar technology innovation, adoption and diffusion.

7. STAFF-RESOURCES

Staff-resources Analytics

do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- ***Man* : human capital management (scientists, business analysts, system analysts, project managers): talent acquisition, talent retention, training, reward and recognition;**
- ***Machine* (tools, electrical and electronic machines, computer hardware, software, internet);**
- ***Material* :Photonic cells;**
- ***Method* : process innovation for manufacturing of solar cells, PV panels and power electronic circuit;**
- ***Money* : (optimal fund allocation, project management, resource allocation, resource distribution**

The expert panel have explored the issue of optimal allocation and distribution of critical resources. It is essential to coordinate various R&D units of renewable energy and Powergrid Corporation, electrical, power electronics, photonics and power plant departments of engineering institutes, technology management department of management institutes and collaborative networks. The team of innovators must have creativity, shared vision, intellectual abilities, thinking style, knowledge, personality, motivation, commitment, confidence and group dynamics.

The intelligent and creative innovators should at this emerging technology in unconventional ways.
The world is enjoying today the evolution of internet and mobile communication technology which is the outcome of hard work, commitment and involvement of the great talents in electronics and telecommunication engineering. Similar type of involvement and commitment is essential from various forums of electrical and electronics engineering, photonics and renewable energy sectors globally. Organizational creativity should be fostered through intelligent human capital management, talent acquisition and retention strategy. The solar power system should be operated and maintained by a pool of intelligent, educated, efficient, productive, committed and motivated workforce. Active involvement, knowledge sharing and optimal human talent utilization is essential for innovation, adoption and diffusion of this emerging technology. The workforce should develop skills in erection, testing, commissioning, operation, maintenance and trading of solar power system. New business model requires the support of an effective human resource management system for talent acquisition and retention, skill development, training, career growth planning, incentive, reward and recognition.

8. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- ***Skill*: technical, system admin, management, legal, governance, surveillance, relationship management;**
- ***Style*: leadership, shared vision, goal setting, intelligent communication protocol, risk assessment and mitigation;**
- ***Support* : proactive, preventive and reactive support.**

The expert panel are also exploring and analyzing *skill-style-support* for energy security. What should be the innovation model for effective diffusion of solar power technology? Is it possible to adopt *K-A-B-C-D-E-T-F model* (Ref. : session 1)? The innovators should develop different types of skills in technical (e.g. photonics, photovoltaic and renewable energy, power plant, power electronics, electrical and electronics), technology management and system administration such as research and development, maintenance support, knowledge management, system design and project management (e.g. erection, testing and commissioning). The system administrators must have multiple leadership skills such as smart thinking, communication, coordination and change management. The workforce should develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of solar power innovation demands the support of effective leadership style. It is really challenging for the project leaders to implement top technology innovations physically and practically. Top management can tackle the complexity of system implementation by developing an efficient team through group dynamics. It is essential to develop skills in development of solar power system through proper

coordination among design, supply and customer chain and R&D, production and marketing functions. The basic objectives are to maximize fit with the needs of the users, ensure quality assurance, minimize time to market, sales and distribution and control product development cost. It may be an interesting initiative to make the suppliers and the users involved in the development process.

The workforce involved in solar power trading should develop different types of skills such as research and development, product design, sales, event management, project management, erection, testing, commissioning and service maintenance. An effective innovation model requires the support of a knowledge repository in the form of a digital library which should extract good up-to-date data from top journals and magazines on solar power electronics and solar energy.

What should be the ideal organization model for solar power trading? A traditional functionally centered organization model may be suitable for supporting end-to-end business processes. The business model of solar power requires the support of a functional structure enabled with advanced information and communication technology. The structure should have project, design, power generation, distribution, maintenance, revenue management, human resource management, supply chain management and finance cells. The business model requires a collaborative and cooperative work culture.

Solar technology management is not a trivial simple problem; it is associated with multiple domains such as electrical engineering, power electronics, materials science, structural engineering, physics, photonics, chemistry, nanotechnology and business analytics. A collaborative platform is essential for effective interaction among national and international technical experts and scientists from industry and academic institutions; energy policy makers, consultants, engineers, technicians, strategists, construction professionals, architects, infrastructure project managers, entrepreneurs, traders, venture capitalists, banking and financial institutions, industrial forums and trade fair committees and organizers. The social media, news channels, radio and TV broadcast are expected to play a responsible role for general awareness of the public and government and promotion of the technology globally.

The diffusion of solar power technology demands the support of great leadership style; they are not only industry leaders but also political one. The style is basically the quality of leadership; the leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. The leaders must be able to share a rational vision, mission and values of solar power system among all the stakeholders honestly and appropriately in time. It is really challenging for the great leaders to implement and build solar power system for global energy security. They have to face and tackle threats from traditional industries such as coal, oil and gas, thermal and nuclear power, selfish local bias, power play and politics. They must understand the intelligence of business modeling and system dynamics associated with solar energy, they must exercise fundamental rethinking and radical redesign of global energy trading system. Top management should be able to tackle the complexity of system implementation through a strong project team, right mix of dedicated technical and business experts.

9. CONCLUSION

The expert panel have explored the potential of solar power through deep analytics. It is clear from scope and SWOT analysis that solar power is a potential option of sustainable energy and business model innovation for the future as compared to other sources of energy. Solar power is at the growth phase of technology life-cycle. The technology is still not matured; there are several constraints such as efficiency of solar cell and cost of solar panels. It is possible to extend the scope of solar power to the battery charging of electric vehicles and drones (Ref. : session 7). It may be very useful and economical to adopt solar power driven water pumps in agriculture, warehouses, cold storages and other innovative applications (Ref.: Session 3) . The ultimate success of any innovation effort no longer depends on a single element alone. It is important to understand the customers and competition and also to recognize and align the critical partners in the innovation ecosystem. It is essential to identify the blind spots of solar technology which are efficient solar cell, power electronics circuit and business model innovation.

FURTHER READING

- **R.H.Waterman, T.J.Peters and J.R. Phillips. Mckinsey & Company. Structure is not organization. Business Horizons. June'1980.**
- **M.W.Johnson, C.M.Chritensen and H.Kagermann. Reinventing your business model. Harvard Business Review. Decmber'2008.**
- **M.Hammer. Process management and the future of six sigma. MIT Sloan Management Review, Vol. 43, No. 2, pp.26–32.2002.**
- **S.Chakraborty and S.K.Sharma. Enterprise Resource Planning: an integrated strategic framework. International Journal Management and Enterprise Development, Vol. 4, No. 5, 2007.**
- **R.Roy. Entrepreneurship. Oxford University Press. 2008.**
- **G.Boyle. Renewable Energy. 2nd Edition. Oxford University Press. 2004.**
- **Department of Energy, USA. Renewable energy: an overview. March'2001.**
- **F.Kreith and D.Y.Goswami (edited). Handbook of energy efficiency and renewable energy. CRC Press. 2007.**
- **B.K.Bose. Power Electronics and Motor Drives. Advances and trends. Elsevier. 2006.**
- **S.K.Mazumder. High-Frequency Inverters: From Photovoltaic, Wind and Fuel Cell Based Renewable and Alternative Energy DER/DG Systems to Energy-Storage Applications. University of Illinois, USA. 2010.**
- **X.Yang, Y.Song, G.Wang and W.Wang. A comprehensive review on the development of sustainable energy strategy and implementation in China. IEEE Transactions on Sustainable Energy, volume 1, no. 2, July'2010.**
- **H.M.Upadahyaya, T.M.Razykov and A.N.Tiwari. Thin film PV Technology. In F.Kreith and D.Y. Goswami (Edited). Handbook of energy conservation and renewable energy. CRC Press, NY,USA. 2007.**
- **T.M.Razykov,B.Rech and A.N.Tiwari (Edited). Special issue on thin film PV. Solar Energy, N6. 2004.**

- **S.B.Kjaer, J.K.Pedesen and F.Blaabjerg. A review of single phase grid connected inverters for photovoltaic modules. IEEE Transactions Industrial Application. Volume 41, no. 5, pp. 1292-1306, Sep / Oct'2005.**
- **ABB online document : Distributed energy storage product presentation. 2010.**
- **U.S. Department of Energy. Solar Energy Grid Integration System Energy Storage (SEGIS-ES).May'2008.**
- **S.J.Chiang, K.T.Chang and C.Y.Yen. Residential photovoltaic energy storage system. IEEE Transactions on Industrial Electronics. vol. 45, no. 3, pp 385-394, June'1998.**
- **R.W.De Doncker, C.Meyer, R.U.Lenke and F.Mura. Power electronics for future utility applications. IEEE 7th International conference Power Electronics Drive System. November'2007.**
- **F. Katiraei, R. Iravani, N. Hatziargyriou and A. Dimeas. Microgrids management. IEEE Power Energy Magazine, vol. 6, no. 3, pp. 54–65, May/Jun. 2008.**
- **M. Marinelli, F. Sossan, G. T. Costanzo and H. W. Bindner. Testing of a Predictive Control Strategy for Balancing Renewable Sources in a Microgrid. IEEE Transactions on Sustainable Energy.**
- **J.Charias. Maxium power solar converter. Microchip.**
- **R.Faranda and S.Leva. A comparative study of MPPT techniques for PV system. 7th WSEAS International Conference on Application of Electrical Engineering, Norway, July,2008.**
- **T.Esram and P.L.Chapman. Comparison of photovoltaic array maximum powerpoint tracking techniques. IEEE Transactions on Energy Conversion. Vol. 22, No.. 2, June 2007.**
- **J.Charais. Maximum power solar converter. Microchip Technology Incorporation. 2010.**
- **RIB, Italy. Solar amplifier. Code ACG9125.**
- **J.Falin and W.Li. A boost-topology battery charger powered from a solar panel. Texas Instruments. www.power.ti.com.**
- **http://www.MitsubishiElectric.com**
- **http://www.tatapowersolar.com**
- **http://www.msme.gov.in**
- **http://www.ediindia.org, www.nabard.org**
- **S. B. Kjaer, J. K. Pedersen, and F. Blaabjerg. A review of single-phase grid-connected inverters for photovoltaic modules. *IEEE Trans. Ind. Appl.*, vol. 41, no. 5, pp. 1292–1306, Sep./Oct. 2005.**
- **S. B. Kjaer, J. K. Pedersen, and F. Blaabjerg. Power inverter topologies for photovoltaic modules-a review. in *Proc. 37th IAS Annu. Ind. Appl. Conf. Meet. Rec.*, 2002, vol. 2, pp. 782–788.**
- **F. Blaabjerg, R. Teodorescu, M. Liserre and A. V. Timbus. Overview of control and grid synchronization for distributed power generation systems. *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1398–1409, Oct.2006.**

- **B. J. Pierquet. *Designs for Ultra-High Efficiency Grid-Connected Power Conversion*. Ph.D. dissertation, Dept. Electric. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, 2011.**
- **P.Sanjeevikumar, E.Kabalci, A.Iqbal, H.Abu-Rub, O.Ojo. Control Strategy and Hardware Implementation for DC-DC Boost Power Conversion Based on Proportional-Integral Compensator for High Voltage Application. *Engineering Science and Technology: An International Journal* (*JESTECH*), Dec.2014.**
- **P.Sanjeevikumar, A.Iqbal, H.Abu-Rub, M.Bishal. Implementation and control of extra high voltage dc-dc boost converter. *7th IET Intl. Conf. on Sustainable Energy and Intelligent System,* IET-SEISCON'13,Chennai, India. 2013.**
- **F.Blaabjerg, F.Iov, T.Kerekes, R.Teodorescu. Trends in power electronics and control of renewable energy systems. *14th Int. Power Electron. & Motion Control Conf.,* 2010.**
- **J. M. Guerrero, F. Blaabjerg, T. Zhelev, K. Hemmes, E. Monmasson,S. Jemei, M. P. Comech, R. Granadino, and J. I. Frau. Distributed generation: Toward a new energy paradigm. IEEE Ind. Electron. Mag., Vol. 4, No. 1, pp. 52-64, Mar. 2010.**
- **R. Lasseter. Smart distribution: Coupled microgrids. IEEE Proc., Vol. 99, No. 6, pp. 1074-1082, Jun. 2011**
- **M. Barnes, J. Kondoh, H.Asano, J. Oyarzabal, G. Venkataramanan, R. Lasseter, N. Hatziargyriou, and T. Green. Real-world microgrids – an overview. Proc. IEEE SoSE, pp. 1-8, 2007.**
- **N. Hatziargyriou, H. Asano, R. Iravani and C. Marnay. Microgrids. IEEE Power Energy Mag., Vol. 6, No. 4, pp. 78-94, Jul./Aug. 2007.**
- **F. Katiraei, R. Iravani, N. Hatziargyriou and A. Dimeas. Microgrids management. IEEE Power and Energy Mag., Vol. 6, No. 3, pp. 54 -65, 2008.**
- **A. Timbus, M. Liserre, R. Teodorescu, P. Rodriguez, and F. Blaabjerg. Evaluation of current controllers for distributed power generation systems. IEEE Trans. Power Electron., Vol. 24, No. 3, pp. 654-664, 2009.**
- **M. Kazmierkowski, R. Krishnan, and F. Blaabjerg. Control in Power Electronics. London, U.K.: Academic, 2002.**
- **N. Pogaku, M. Prodanovic and T. Green. Modeling, analysis and testing of an inverter-based microgrid. IEEE Trans. Power Electron., Vol. 22, No. 2, pp. 613-625, 2007.**
- **P. Kundur, Power system stability and control. New York: McGraw-Hill, 1994.**
- **J. Lopes, C. Moreira and A. Madureira. Defining control strategies for microgrids islanded operation. IEEE Trans. Power Syst., Vol. 21, No. 2, pp. 916-924, May 2006.**
- **M. H. Nehrir, C. Wang, K. Strunz, H. Aki, R. Ramakumar, J. Bing, Z. Miao, and Z. Salameh. A Review of Hybrid Renewable/Alternative Energy Systems for Electric Power Generation: Configurations, Control, and Applications. *IEEE Trans. Sustain. Energy*, vol. 2, no. 4, pp. 392–403, Oct. 2011.**

- K. Kurohane, T. Senjyu, A. Yona, N. Urasaki, T. Goya, and T.Funabashi. A hybrid smart AC/DC power system. *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 199–204, 2010.
- K. T. Tan, P. L. So, Y. C. Chu, and M. Z. Q. Chen. Coordinated Control and Energy Management of Distributed Generation Inverters in a Microgrid. *IEEE Trans. Power Delivery*, vol. 28, no. 2, pp. 704–713, Apr. 2013.
- C. T. Rodríguez, D. V. de la Fuente, G. Garcerá, E. Figueres, and J. A. G. Moreno. Reconfigurable Control Scheme for a PV Microinverter Working in Both Grid-Connected and Island Modes. *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1582–1595, Apr. 2013.
- Sh. Jiang, W. Wang, H. Jin, and D. Xu. Power Management Strategy for Microgrid with Energy Storage System. in *Proc. 2011 IEEE IECON- 37th Annual Industrial Electronics Society Conf.*, pp. 1524-1529.
- International Standard for Testing Solar Cookers ASABE Standard S580 Dr. Paul A. Funk, Avinashilingam University, Coimbatore, India, January 1997.
- S. C. Mullick, T. C. Kandpal, and A. K. Saxena. Thermal test procedure for box-type solar cookers,*Solar Energy*, vol. 39, no. 4, pp. 353–360, 1987.
- S. K. Philip and H. N.Mistry. Solar cooker testing: a suggestion for change in BIS standards. *SESI Journal*, vol. 5, pp. 17–22,
- 1995.
- S. K. Philip, T.K.Chaudhuri and H. N.Mistry. Testing of solar box cookers, in *Proceedings of the 3rd International Conference on Solar Cookers Use and Technology*, Coimbatore, India, 1997.
- S. B. Joshi and A. R. Jani. Photovoltaic and Thermal Hybridized Solar Cooker. Hindawi Publishing Corporation ISRN Renewable Energy Volume 2013, Article ID 746189.
- http://www.indiawaterportal.org accessed on 15.08.2018
- http://mnre.gov.in/file-manager/UserFiles/Schemefor-Solar-Pumping-Programme-for-Irrigation-and-Drinking-Water-under-offgrid-and-Decentralised-Solar-applications.pdf accessed on 15.08.2018.
- Trombly, J. Technology solutions: Nano-PV set to accelerate solarenergy use. *Environ. Sci. Technol.*, 38, pp. 376–376A, 2004.
- Catchpole, K. R. Nanostructures in photovoltaics. *Phil. Trans. Math. Phys. Eng. Sci.*, 364, pp. 3493–3503, 2006.
- Tsakalakos, L.Nanostructures for photovoltaics. *Mater. Sci. Eng*., 62(6), pp. 175–189, 2008.
- Green, M. Silicon photovoltaic modules: A brief history of the first 50 years. *Prog. Photovolt.*, 13, pp. 447–455, 2005.
- Jadhav, M. V., Todkar, A. S., Gambhire, V. R., and Sawant, S. Y.. Nanotechnology for powerful solar energy. *Int. J. Adv. Biotechnol. Res*.,2, pp. 208–212, 2011.
- Honsberg, C. B., Barnett, A. M., and Kirkpatrick, D.. Nanostructured solar cells for high efficiency photovoltaics. in *Photovoltaic Energy Conversion, IEEE 4th World Conference*, Hawaii, USA, 2006.

- Nozik, A. J. Nanoscience and nanostructures for photovoltaics and solar fuels. *Nano Lett*., 10(8), pp. 2735–2741, 2010.
- Green, M. A., Emery, K., Hishikawa, Y., and Warta, W. Solar cell efficiency tables (Version 34). *Prog. Photovolt. Res. Appl.*, 17, pp. 320–326, 2009.
- Goetzberger, A., Hebling, C., and Schock, H.. Photovoltaic materials, history, status and outlook. *Mater. Sci. Eng. R Rep.,* 40, pp. 1–46, 2003.
- Banerjee, S., Misra, M., Mohapatra, S. K., Howard, C.. Mohapatra, S. K., and Kamilla, S. K., Formation of chelating agent driven anodized TiO2 nanotubular membrane and its photovoltaic application. *Nanotechnology*, 21, pp. 145201, 2010.
- Jadhav, M. V., Todkar, A. S., Gambhire, V. R., and Sawant, S. Y. Nanotechnology for powerful solar energy. *Adv. Biotech*. *Res*., 2(1),pp. 208–212, 2011.
- Energy and Environmental Science,
- Advanced Energy Materials,
- Progress in Photovoltaics: Research and Applications,
- Annual Review of Chemical and Bimolecular Engineering,
- Nano Energy, Renewable and Sustainable Energy Reviews,
- IEEE Transactions on Sustainable Energy,
- IEEE Transactions on Power Electronics,
- Polymer Reviews,
- Solar Energy Materials and Solar Cells,
- Solar Energy,
- Renewable Energy,
- Environmental Research Letters,
- IET Renewable Power Generation
- Journal of Photonics for Energy.

QUIZ

- Explain the technology of solar power from the perspective of energy security. Justify it as a technology for humanity. What is the scope and emerging applications of this technology?
- What is the dominant design of solar power system?
- What are the basic elements of the system architecture?
- What do you mean by technology security? How to verify the security intelligence?
- What are the strategic moves of technology innovation, adoption and diffusion for solar power? What is the outcome of technology life-cycle and SWOT analysis?
- How to manage resources for this innovation project?
- What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?
- How to manage technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among ‘7-S’ elements?

- **Discuss the evolution of nanotechnology for solar cells.**
- **Design an intelligent power electronic circuit for solar power system.**

APPENDIX:

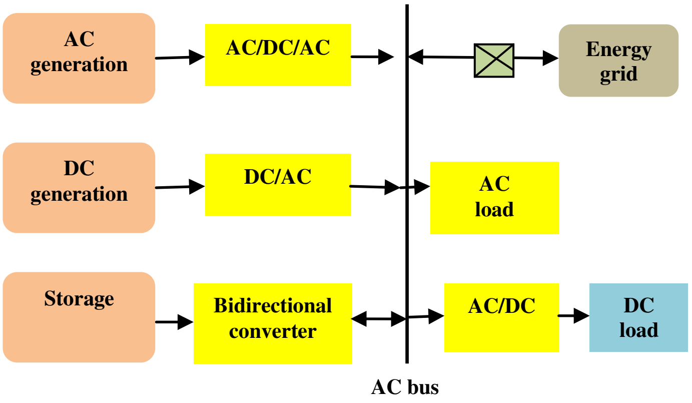


Figure 6.8 (a): AC coupled hybrid microgrid

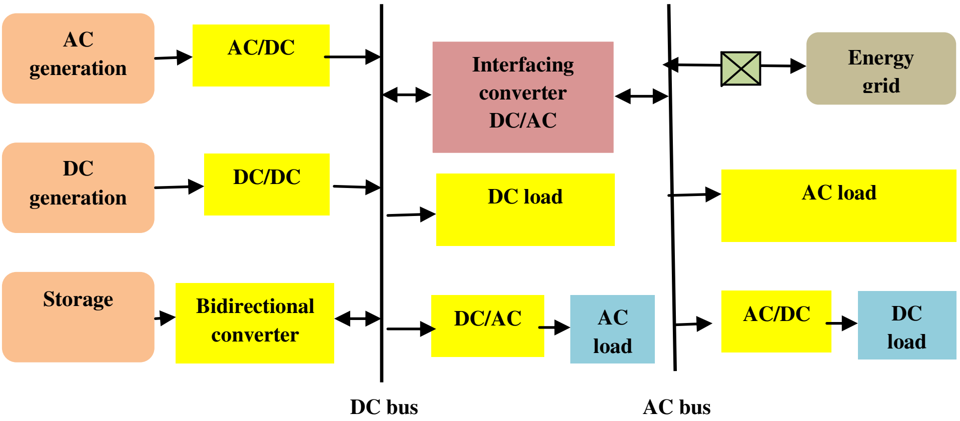


Figure 6.8 (b): DC coupled hybrid microgrid

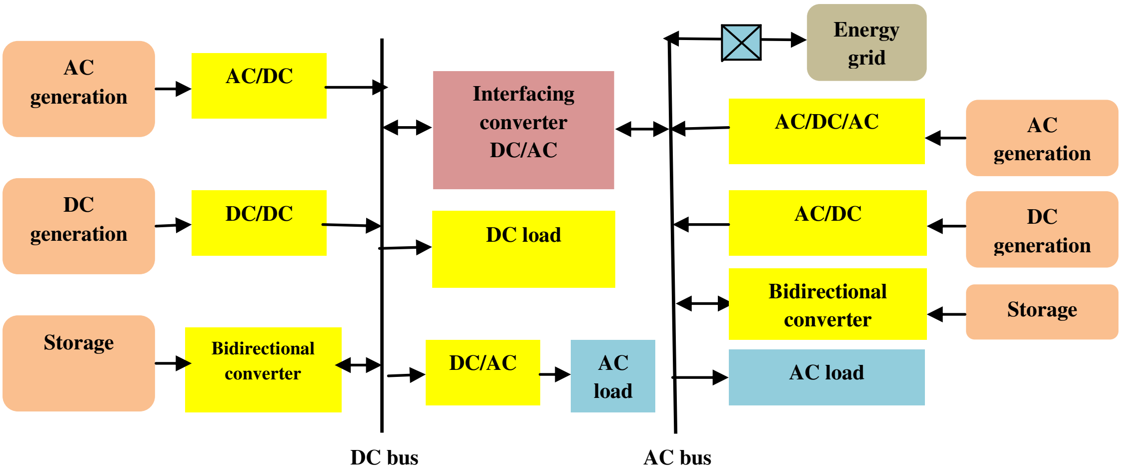


Figure 6.8 (c): AC-DC coupled hybrid microgrid

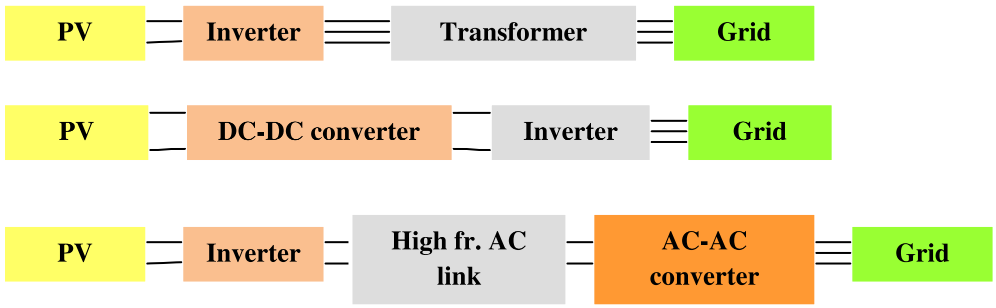


Figure 6.9 : (a) single stage and (b,c) two-stage power conversion system for PV system

Comparison parameters	*AC coupled hybrid microgrid*	*DC coupled hybrid microgrid*	*AC-DC coupled hybrid microgrid*
Topology	DGs and SEs are connected to AC bus through interfacing converters.	DGs and SEs are connected to the common DC bus, and an Interfacing Converter (IFC) is used to link the DC and AC buses.	DGs and SEs are connected to DC and AC buses, where these buses are linked by Interlinking Converter (ILC); most promising microgrid structures in the near future.
Complexity of structure	Simple, dominant structure, multiple port converters may be used.	Simple structure; multiple-port power converters may be used	Complex structure
Operation mode	Stand alone and grid connected ; transition between two modes should be seamless and smooth.	Stand alone and grid connected	Stand alone and grid connected
Control strategy	Simple, the power control can be realized by current or voltage control.	Complexity : medium; central control scheme, uses optimization techniques to adjust set-points of each source.	Complex, Requires high coordination for voltage and power control between AC and DC subsystems; focus on DC and AC bus voltages and frequency control, power balance within DC and AC subsystems
Power management strategy	Grid connected operation mode : dispatched and undispatched output power; standalone : ac bus voltage and frequency control	Complexity : medium; Grid connected operation mode : dispatched and undispatched output power; standalone mode : ac and dc bus voltage control	Complexity : high; Grid connected operation mode : dispatched and undispatched output power; standalone mode : ac and dc bus voltage control

Cost	**May be cost effective**	**May be cost effective**	**May be slightly costly**
Benefits	**Cleanness, simple technologies, increasing demands for electrical energy and exhaustible nature of fossil fuel demands efficient solar microgrids.**	**Emerging new semiconductor devices use silicon carbide and gallium nitride for improved performance of power electronic switches.**	**Higher flexibility and reliability, improves overall efficiency and reduces the system cost with reduced number of power converters**

Table 6.1 : Comparison of power management strategies

SESSION 7: LOGISTICS SECURITY - ELECTRICAL & HYBRID VEHICLES, SMART BATTERIES, RAILTECH SECURITY & DRIVER ADVICE SYSTEM

***Event* : Technology for humanity and global security summit**
***Venue*: Logistics security hall, Technology park: Sanada**
***Time Schedule* : 10 a.m. – 12 p.m., 17.8.2020**
***Agents* : Representatives of various global organizations, Technology management experts from science and technology forums, Logistics engineers, scientists, business development consultants of logisctics industries.**
***Topic of discussion and key focus areas* : Logisctics security, Electrical vehicles, Hybrid vehicles, Smart batteries, Smart transformers, Battery charging mechanism, Solar power, Security and safety, Mobile communication, IoT, RailTech, Driver Advice System, Traffic control Centre, Real-time fault diagnostics, Fault tree analysis, FMEA, Time Failure Propagation Graph (TFPG), Control flow, Resource flow, Data flow**
***Keynote speakers* : Prof. D. Jones, Dr. Simon Rodrigues, Dr. Andy Richardson, Prof. R. Prakash, Prof. B. Williams, Dr. S.Yokoo**

1. SCOPE

Scope Analytics

***Agents*: system analysts, business analysts, agriculture scientists, engineers;**
***Stakeholders* : Drivers, Traffic controller at TCC, passengers;**
***Moves* : critical success factors analysis, requirements management;**
***Application domains* : surface, rail, water, air transport;**
***Key technologies* : mechanical, aeronautical, electrical, electronics, communication; Civil infrastructure (roads, ports, airport, rail stations);**
***Security parameters*: define a set of sustainable development goals for logistics security.**

- ✪ **Logistics security (travel, hospitalities, surface, water, rail, water, EVs and hybrid vehicles)**
- ✪ **Responsible consumption and production (fuel, vehicles)**

Requirements engineering for dominant design of future generation vehicles :

- **Electrical & hybrid vehicles through smart, clean and solar micro grid**
- **Vehicle-to-Vehicle (V2V) communication**
- **Internet of Things (IoT), mobile communication**

***Objectives*:**

- **safe driving trading-off cost vs. comforts of the passengers through real-time fault diagnostics**
- **maintain schedule of train service approximately as far as possible**
- **improve energy efficiency of driving as per standard operating procedures**
- **optimal capacity utilization of limited rail infrastructure**
- **optimize train movements within limits and regulatory compliance**

- **ensure security, safety and comforts at optimal cost**

***Constraints* : Technological complexity, application integration, cost;**

Prof. Jones and Dr. Yokoo have started this session through scope analytics. Sustainable transportation infrastructure demands widespread adoption of electric vehicles (EVs) and renewable energy sources. The use of EVs is growing due to increasing technological success of complex and reliable hybrid vehicles; technological diffusion of Li-ion batteries and increasing willingness of society, political world and the automobiles market due to increasing environmental air pollution, global warming and fuel consumption and high stress on the storage of fossil fuels. This session analyzes the technological innovation of electrical and hybrid vehicles through deep analytics. The dominant design includes smart batteries.

Prof. Jones has outlined the scope of the technological innovation on electrical vehicles which includes E-bus, E-truck, E-scooter, E-bike, E- bicycle, E-Taxi and E-private car. The scope can be extended to E-steamer/ launches / ships, electric trains (e.g. metro rail, mono rail, local trains) and small aircrafts (e.g. helicopters, hovercrafts, fighter planes, military aircrafts, HY4 plane free of carbon emission and driven by serial hybrid powertrain such as fuel cell and alternative energy sources like solar cell). It is interesting to develop power management system of the aircrafts which select appropriate energy sources as per the demand of aircraft and the propeller engine. Vehicles can be powered by internal combustion engine using gasoline, diesel or gas or electric drives. The critical success factors of vehicle manufacturing industry are sustainable, environment friendly design, improvements in power train systems, fuel processing and power conversion technologies.

Vehicles can be classified based on various types of synthetic fuels such as hydrogen, biodiesel, bioethanol, dimethylether, ammonia and electricity via electrical batteries : conventional gasoline vehicle (petrol or diesel, ICE), hybrid vehicle (gasoline fuel, electrical drive, rechargeable battery), electric vehicle (high capacity electrical battery, electrical drive), hydrogen fuel cell vehicle (high pressure hydrogen fuel tank, fuel cell, electrical drive), hydrogen internal combustion vehicle (high-pressure hydrogen fuel tank and ICE) and ammonia fueled vehicle (liquid ammonia fuel tank, hydrogen-fueled ICE). In case of electrical or hybrid vehicles, electricity may be produced from renewable energy sources or natural gas.

It is an interesting option to perform a comparative analysis among various type of vehicles based on a set evaluation parameters such as vehicle price, fuel cost, maintenance cost, economic attractiveness, driving range, energy and power features, safety, sustainability, fuel consumption, reduction in emission and environmental impact. The trading agents often try to trade-off miscellaneous critical factors such as vehicle performance, improved performance of fuel cell or batteries, cost, governmental subsidies and environmental pollution issues. It has been found that hybrid and electrical vehicles have many advantages than other types of vehicles in terms of high fuel price and environmental pollution, economics and environmental impact depends significantly on the source of electrical energy. If the electricity is generated from renewable energy sources, electric car is even better

than hybrid vehicles. Nickel metal hydride and Li-ion batteries have shown improved performance as compared to old lead-acid batteries.

Next critical issue is requirements engineering of vehicles : What should be the vision for the vehicles in future ? The requirements should be defined from several perspectives. It is essential to transform the design principles of the conventional vehicles. The traditional design is based on petrol and diesel engines for energy, internal combustion engine for power, manual control and independent standalone operation. The vision for the future vehicles may be based on electrical and hybrid system, light, clean, safe, fun and fashionable design, mobile communication, and Internet of Things (IoT). The design of the vehicles should promote mobile Internet and IoT enabled by electronic tags and sensors and seamless connection to IoT; the basic objectives are efficient traffic management and reduced travel time by collecting, processing and sharing big data. The electrical and hybrid vehicles should be integrated with smart power grid having clean renewable energy sources (e.g. solar, wind and hydroelectric power), dynamic pricing mechanism and optimal balance between supply and demand of electrical energy. The vehicles should be designed with real-time control capabilities, mobile connectivity and onboard intelligence for optimal utilization of road and parking space and traffic congestion control.

The automobiles market demands fundamental rethinking, radical redesign and reinvention of vehicles of the future. The enabling technologies should be developed in terms of dominant design and converged for proper diffusion of electrical and hybrid vehicles globally. The expected benefits of converging innovative solutions should be explored in terms of lower cost, sustainable economic growth and prosperity, enhanced freedom, mobility, safety, zero emissions, use of clean renewable energy to fight against air pollution, climate change and global warming, minimal traffic congestion, increased roadway throughput, fun, entertainment and autonomous driving.

Prof. Jones is also presting the scope of RailTech, an emerging technology in rail operation from the perspectives of intelligent management information systems. RailTech integrates intelligent Driver Advice System (DAS), traffic control centre (TCC) and real-time fault diagnostics (RTFD). The complexity of the technology has been analyzed through deep analytics. The basic building blocks of real-time fault diagnostics are graphical analytics (GA), fault tree analytics (FTA) and failure mode effects analytics (FMEA). The core components of the graphical analytics include time failure propagation graph (TFPG), control, resources and data flows analytics. What should be the top priority: high speed train or rail security and safety? The emerging technology should adopt a balanced approach.

RailTech integrates Driver Advice System (DAS), traffic control centre (TCC) and real-time fault diagnostics (RTFD) for rail operations. RailTech is analyzed based on literature reviews on rail safety, driver advice systems and real-time fault diagnostics from the perspectives of management information systems (MIS), extensive experience of rail travel of more than 100000 kilometers in last twenty five years and also training experience at Railways Corporation.

The ultimate goals of RailTech are to improve the performance of rail infrastructure and train services and minimize train delays which results decrease

in capacity utilization, punctuality, reliability and safety. Increased capacity of infrastructure also causes secondary delays and increase in route conflicts. It is essential to do analysis on various types of feedback and operational data for improving planning and control in rail operations and to monitor delays at stations using route conflicts, train and timetable data. Specifically, RailTech faces critical situations during natural disasters (e.g. flood, cyclone, storm, fog, mist and snowfall in winter). Deep analytics can find out chains of route conflicts, secondary delays, number of conflicts, time loss and delay jump.

RailTech safety and security is an emerging trend of top technological innovation today. Railway technology is associated with a complex, distributed and integrated information system. We must monitor the performance of railways infrastructure globally and analyze political and social trends, principal technological advancement of condition monitoring system, driver advice system and real-time fault diagnostics; system complexity, R&D challenges and future vision of railway security and safety.

Condition monitoring is an important issue of RailTech safety. It is a common practice to compare relative benefits and limitations of various modes of transportation such as surface, rail and air in terms of traffic congestion, environmental pollution, safety, reliability, consistency, cost and capacity utilization. Traditionally, the security and safety of RailTech system is analyzed in terms of frequency of accidents, fire hazards, delay, punctuality, reliability, consistency, probability of injuries or fatalities due to derailing and track faults. Gradually, the system has been getting equipped with electronics, communication and information technology which increases the scope of automated fault detection and diagnosis. It is possible to improve punctuality, profit and revenue in rail operations and increase operational availability and reliability of key railway infrastructure through effective coordination and integration among DAS, TCC and RTFD.

2. SYSTEM

System Analytics

***Agents*: system analysts, business analysts, scientists, engineers;**
***Moves* : requirements engineering, system design, prototype testing, production, erection, testing, commissioning;**
RailTech System Intelligence

- **advise a train driver the target arrival time along a specific route to satisfy the timetable and avoid conflicts with other trains;**
- **monitor the train's speed so that the advice is updated correctly and target time of the train is achieved;**
- **compute energy efficient speed/distance profile to achieve target time;**
- **advise a driver conflict free time target i.e. how far and fast a train can be driven safely within allocated and authorized movement hiding wider view of overall traffic management of rail network.**
- ***Computing schema***
    - **track train movement**

  - **predict future train movement**
  - **conflicts detection and resolution**
  - **new target train timings to avoid conflicts**
  - **speed profiles and choice of advice to the driver**
- ***Networking schema***
  - **3G/4G/5G to DAS with built-in antenna**
  - **3G/4G/5G with external antenna**
  - **3G/4G/5G to a communication gateway onboard**
  - **Data communication via SMS**
- ***Data schema***
  - **Explicit driving instructions : current speed target, time series analysis of train speed profile, advice to speed up or slow down;**
  - **Temporal information : train running status (early / delay), optimized speed profile to realize time table;**
  - **Decision support information : gradient profile, energy usage, position of other trains, conflict, traffic congestion;**
  - **Data mining: monitor a set of performance metrics such as primary and secondary delays, capacity utilization, route conflicts, traffic congestion, signaling errors and real-time train scheduling and time table.**
- ***Application schema* :**
  - **Provide advice to the train driver for running the train in a safe and efficient manner;**
  - **Collect and recall from route knowledge the current and future speed targets such as infrastructure, regulation and operational factors;**
  - **Select correct train speed to minimize delay and maximize safety;**
  - **Monitor the speed of the train by collecting data from sensors, speedometer, noise and motion;**
  - **Compare correct speed with train speed and compute speed gap;**
  - **Speed control to minimize the difference between target required speed and actual train speed by changing the setting of the power or brake controller and considering train's response, gradients, curves and professional driving policy;**
  - **Assist the driver to monitor the progress of a train continuously against a series of scheduled stops and understand if the train runs early or late between two timing points;**
  - **Advice for any temporary speed restrictions within a route to give a perception of progress and recovery time to the driver;**

Prof. B. Williams and Dr. Andy Richardson are presenting system analytics for electrical and hybrid vehicles and railways technology. BEVs are the simplest type of EV using electrical power from a single source of battery to power one or more electric motors. A single electric motor is connected to the front axle through a simple gearbox; a series of four hub motors may be attached to each wheel. The battery has many cells combined into modules and the modules are grouped into packs through series and parallel connections. For example, 100 Li-ion series

connected batteries with cell voltage of 3.6V can produce 360 V. The battery pack is the largest and most expensive component of the BEV; it is readily removable and swappable. Typically, EVs have higher initial costs, lower fuel costs, lower external costs, higher insurance costs, lower maintenance and repair costs. The cost of EV system depends on various types of elements such as size of key components (e.g. batteries, fuel cells, electric motors), desired performance, driving range, energy efficiency, cost of key materials for EV components (e.g. Li for batteries, platinum for fuel cells and carbon fiber for pressure vessels), life-cycle of key components, the impact of technological learning and economies of scale on manufacturing cost, energy use of EV, technology, design of the power train, drive cycle and weight; cost of energy (e.g. fuel production, distribution and delivery costs), insurance and maintenance cost.

There are various types of battery charging methods such as normal, induction, semi-fast and fast charging. Normal charging uses standard domestic socket, can be used anywhere but is limited in power. Semi-fast charging allows a higher charging power (up to 22 kW), suitable for most EVs. Fast charging needs a more expensive infrastructure. Inductive charging does not use plugs and cables and suitable for specific applications. The basic requirements of the technological innovation of EVs include availability of efficient electric energy storage devices or batteries and recharging infrastructure to transfer electric energy from the distribution grid to the battery.

EVs may also need intelligent communication protocol for vehicle identification and billing, charge cost optimization and grid load optimization. Typically, NCA (Li-Ni-Co), NCM (Li-Ni-Mn), LMO (Li-Mn spinel), LTO (Li-Titanate), Li ion Phosphate (LFP) technologies are used to make EV batteries. It is possible to do a comparative analysis of various types of batteries based on materials of anodes and cathodes, safety, performance,, cost, life-span, specific energy and specific power. The value chain associated with electrical vehicles has various processes such as component production, cell production, module production, pack assembly, vehicle integration, use, reuse and recycling.

Value chain analysis of EV batteries

- **Component production : cathode, anode, binder, electrolytes, separator, active materials**
- **Cell production : single cell assembly**
- **Module production: cells into larger modules**
- **Pack assembly: install modules together with power charging & temp.**
- **Vehicle integration: Integrate battery pack into vehicles battery car interfaces, plugs, mounts**
- **Use : Use during battery life -time**
- **Reuse & recycle: Cleaning and deconstruction**

***Smart Batteries*: Smart batteries are essential part of the dominant design of electrical and hybrid vehicles; Smart batteries should have higher energy density and tolerance to higher temperatures; should avoid the use of dangerous toxic materials, should be nonflammable and safe to use and should withstand higher voltage. Smart batteries are expected to be simple in design, cheaper and lighter in**

weight as compared to present batteries; won't need liquid cooling; the batteries should be long lasting, fire-proof and should permit faster charging. Existing battery technology for EVs is very expensive and has limitations in terms of poor system performance at low temperature, impact of pressure, breakage due to mechanical stress and risks of dendrites.
EVs can be classified into non-hybrid vehicles (ICE) drive), hybrid electric vehicle (micro, mild, full, plug-in), extended range EV (EREV), BEV and fuel cell electric vehicle (FCEV). The hybrid solution obtains reduction of consumption and emissions; heat engines are operated more efficiently; electric power accumulators and electric motors allow energy recovery during braking and its use for traction purposes. In case of series hybrid vehicles, the electric motor supplies power to the wheels. In case of parallel hybrid vehicles, both the heat engine and the electric motor supply power to the wheels. In case of series-parallel hybrid vehicles, the heat engine can drive the wheels directly. It is an interesting agenda to do a multidimensional comparative analysis on various types of batteries (e.g. Li-Ni-Co-Al, Li-Ni-Mn-Co, Li-Mn, Li-Mn-P.,. Li-Ti) based on six dimensions – life span, cost, specific energy, specific power, dafety and performance.

Electrical Vehicle's Battery Charging Mechanism

Let us analyze the battery charging mechanism of electrical and hybrid vehicles. The basic objective is to develop an efficient market mechanism or market interface where the trading agents i.e. the service consumers of electrical vehicles and the service providers of battery charging stations act rationally and negotiate a flexible and intelligent service contract on the replenishment of charged batteries based on approximate estimation of their preferences in EV charging scenario. The market mechanism is expected to maximize the utilities of the trading agents through efficient resource allocation subject to the constraints of time and cost and limited supply of electrical energy. Traditional auction mechanism may not be an interesting option in this business model.

***Agents* : Service consumer (B), Service provider (S);**
***Input*: Demand plan of B, Supply plan of S;**
***System*: Electrical / hybrid vehicles, batteries, battery charging stations,**
***Objectives*: minimize mismatch between demand and supply plans of charged batteries;**
***Constraints*: time, cost, technology;**
***Strategic moves* : Select optimal resource allocation heuristics - FCFS (First Come First Served), Most Requests First (MRF), Longest Waits First (LWF), Selective resource allocation for emergency load (linear / proportional allocation);**
***Protocol:* The agents settle single or multiple intelligent service contracts.: Collaborative planning, forecasting and replenishment (CPFR), Swing option, Push pull, Group buying;**
***Payment function*: verify business intelligence of service contracts in terms of (pay per use, payment mode, payment terms);**

***Security intelligence*: verify security intelligence in terms of rationality, fairness, correctness, transparency and accountability; B and S preserve privacy of SC contract as per revelation principle;**
***Output*: Battery charging service contract.**

Collaborative planning, forecasting and replenishment (CPFR) is a strategic tool for comprehensive value chain management. This is an initiative among all the stakeholders of the supply chain and service chain in order to improve their relationship through jointly managed planning, process and shared information. The ultimate goal is to improve the position of the battery charging service provider in the competitive market and the optimization of its own value chain in terms of optimal inventory, improved sales, higher precision of forecast, reduced cost and improved reaction time to customer demands. The interplay between trust and technology encourages the commitment of collaboration among the trading agents.

Let us consider a specific scenario of multi-party negotiation in battery charging of electrical vehicles. *Swing option* is a specific type of supply contract in trading of stochastic demand of a resource such as charged battery for electrical / hybrid vehicles. It gives the owner of the swing option the right to change the required delivery of a resource through short time notice. It gives the owner of the swing option multiple exercise rights at many different time horizons with exercise amounts on a continuous scale. A typical swing option is defined by a set of characteristics and constraints. There are predefined exercise times t_i, i $\in$[1,2,..,n], 1≤ t_1≤t_2…≤t_n≤ T at which a fixed number of d_0 units of a resource may be obtained. With a notice of specific short period, the owner of the option may use swing right to receive more (up-swing) or less (down-swing) than d_0 at any of n moments. The scheme permits swing only at g out of possible n time moments where g ≤ n is swing number constraint. A freeze time constraint forbids swings within short interval of the moments. The local constraints up-swing [α] and down-swing limits [β] define how much the requested demand d_i at time t_i may differ from d_0. There are two global constraints which restrict the total requested volume D within the contract period by maximum total demand (γ) and minimum total demand (λ). The option holder must pay penalty determined by a function for violating local or global constraints. In this contract, the primary negotiation issue may be a discriminatory pricing plan which depends on the negotiation of a set of secondary issues such as up-swing limit, down-swing limit, maximum total demand, minimum total demand, penalty function and number of swings for a specific period.

Dr. Richardson is discussing various critical issues of railtech system. The system should be designed to satisfy multiple objectives subject to various constraints. The system should have clearly defined objectives, decision making procedures and quantitative measures of performance. The state of the system at a specific time is a set of properties of the system. RailTech system is a complex grouping of interlinked components; it can be decomposed into a set of interacting schema such as computing, networking, data, application and security schema. Each schema can be outlined as stated above. DAS is basically an information system. The basic building blocks of the computing schema are a set of algorithms which compute critical system parameters. The networking schema is the communication system. The data

schema processes data collected by the sensors and various measuring instruments. The application schema defines the basic features of driver advice system. The complexity of the system should be analyzed in terms of number of interacting elements, number of relationships among the elements, number of objectives and number of ways the system interacts with internal and external environment.

3. STRUCTURE

Structure Analytics

RailTech System Architecture

- **Driver advice system**
  - **Option 1 : DAS at TCC (Traffic Control Centre) /* refer figure 7.1*/**
  - **Option 2 : DAS Task shared between TCC and train /* refer figure 7.2*/**
  - **Option 3 : DAS tasks mainly onboard /* refer figure 7.3*/**
- **Railway system**
  - **track side infrastructure**
  - **vehicle or rolling stock**
- **Railway infrastructure assets**
  - **mechanical actuators (e.g. point machines, level crossing barriers, train stops, mechanical signals);**
  - **power supply equipment (e.g. substations, rectifiers, transformers);**
  - **track (e.g. rail, pads, sleepers, ballast, substructure);**
  - **signaling and telecoms (e.g. track circuits, interlockings, axle counters);**
- **Railway rolling stock**
  - **bogie : wheels, axles, suspension components;**
  - **traction and braking systems: motors, power electronics system, transformers, brakes;**
  - **auxiliary subsystems : doors; air conditioning system;**
  - **train communication bus (integrating the subsystems to a central controller);**

Dr. Williams is focusing on the structure of emerging technologies related to logistics security. The new automotive DNA is expected to be developed through proper integration of electrical drives and connected vehicle technologies. The design principles are based on electrical drives with electrical motors for power, renewable solar energy for battery charging and electronic systems for control. Hybrid EVs may use batteries and electric motors to improve the efficiency of mechanically driven vehicles. Smart vehicles are expected to be lighter, more conducive to electrical drives and renewable sources of energy to avoid air pollution. The computing schema should be able to estimate price and incentives for regulating demand and supply of electrical energy. Smart vehicles should be able to communicate wirelessly with each other and with roadway infrastructure and activities through global positioning system (GPS) technology and digital maps. Intelligent vehicle-to-vehicle (V2V) communication protocols should be able to avoid collision and crashes.

SL No.	Structural components	Technology schema
1.	Mechanical system	Mechanical components, transmission, brakes
2.	Electrical & Electronics system	Power supply, battery charger, batteries, inverter, motor
3.	Battery charging station	Normal, induction, fast and semi-fast charging
4.	Information & communication technology	Digital transformation : Computing, networking, data, application and security schema, intelligent communication protocol

Table 7.1 : Structural analysis of electrical and hybrid vehicles

The *topology* of smart vehicles has been analyzed in terms of a set of sub-systems or modules, connectivity, type of connections, layers, interfaces between layers and organization of layers. The structure of EVs has three major components: mechanical system (e.g. brakes, wheel), electrical and electronics system (e.g. battery charging) and information & communication systems (e.g. driver advice system) [Table 8.1]. The sensors collect data from various systems and provide the inputs to DAS. DAS analyzes the sensed data and shows the output (e.g. alerts, advice) to the driver. Figure 8.5 shows typical structure of a hybrid EV.

It is essential to adopt a new automotive DNA which can transform the design principles of smart vehicles. The structure of traditional vehicles is mechanically driven and powered by ICE, energized by petrol and diesel, mechanical control system and operated in standalone mode. The new structure is expected to be more flexible, automated and simple to use. Another important part of the structure is mobile Internet; it is the backbone of communication schema which should enable the vehicles to share real-time and location-specific big data for optimal traffic management, minimal and more predictable travel time and no distraction of driving. The vehicles should be integrated with IoT and may be considered as nodes in mobile networks. The structure is expected to be less expensive to own and operate and should have light weight and less space. The integration of a set of transformative ideas should optimize the benefits, positive impacts and side effects in terms of design direction, energy, environment, safety, congestion and access inequality. These enabling technologies have been getting matured and converged gradually for practically feasible and large scale production. Common components of hybrid vehicle are power supply, normal, onboard and quick charging system, drive battery, inverter, motor, transmission and driving, regenerative braking and electricity generation system.

***Smart Batteries*: Smart batteries are an essential part of electrical and hybrid vehicles; let us explore and analyze the scope, system, security and strategy of smart batteries for EVs. Solid State Batteries (SSB) may be the future of EVs. Alternatively, EVs can use batteries having Li-ion, Ni-metal hydride (NiMH) and electric double layers ultra capacitors led by Li-ions. SSB is an emerging technology**

that uses solid electrodes and solid electrolyte such as ceramics (oxides, sulfides and phosphates), glass and solid polymers. Solid state batteries are safer with higher energy densities but at higher cost. Li-ion batteries use liquid or polymer electrolytes. SSB is generally used in pacemakers, RFID and wearable devices. Presently, the technology of SSB is being developed at Tesla, Toyota, Dyson (Sakti 3), Caterpillar (Fisker), Swiss Fraunhofer institute, Cambridge University; the technology has been diffusing globally. Toyota has planned to use solid state batteries in EVs by 2020. The challenge is to explore a solid conductive material fit for large batteries. Solid Power and Volkswagen are also investing to build high capacity manufacturing plants of SSB.

The next interesting issue is structure of RailTech system. The topology of technology should be analyzed in terms of nodes, connectivity, type of connections, layers, interfaces between layers and organization of layers. RailTech structure has three major components: trackside infrastructure, rolling stock or vehicle and driver advice system. Dr. Williams and Dr. Yokoo are giving the basic overview of rolling stock, infrastructure and the outcome of SWOT analysis of various types of DAS architectures. The sensors collect data from the track and rolling stock and provide the inputs to DAS. DAS analyzes the sensed data and shows the output (e.g. alerts, advice, recommendations) to the driver and traffic control centre (TCC).

***SWOT Analysis on various DAS architectures* : It is essential to analyze strength, weakness, opportunities and threats of RailTech innovation. There are opportunities of growth of the technology in various types of train services such as metro rail, local train and long distance train. But, the technological innovation may face various types of threats such as complexity, integration and digital transformation through sensors, information and communication technologies. It is hard to integrate the mechanical and information systems physically. Let us analyze three different types of system architectures in figures 7.1, 7.2 and 7.3. We have extended these architectures by incorporating the concept of real-time fault diagnostics. In each system architecture, the basic building blocks of RTFD are three analytics i.e. graph analytics (GA), fault tree analytics (FTA) and failure mode effects analytics (FMEA); the output of these analytics is fed to DAS. The core components of GA include control, resources and data flow analytics. In figure 7.1, DAS intelligence is deployed at TCC and the onboard system only displays advice information to the driver. The system can be implemented using existing driver interface without any additional system in the train. But, the scope of data displayed and dynamic update of compensating feedback to the driver is limited. This is an interesting practical and economic solution for possible DAS rollout in future.**

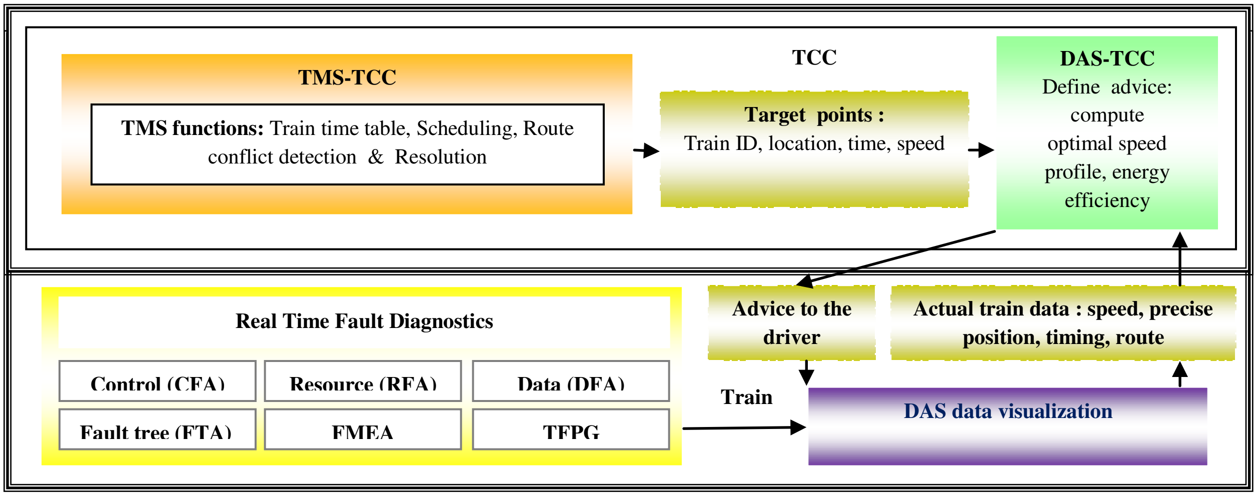

TMS-TCC
TMS functions: Train time table, Scheduling, Route conflict detection & Resolution
TCC
Target points : Train ID, location, time, speed
DAS-TCC
Define advice: compute optimal speed profile, energy efficiency
Real Time Fault Diagnostics
Control (CFA)
Resource (RFA)
Data (DFA)
Fault tree (FTA)
FMEA
TFPG
Advice to the driver
Actual train data : speed, precise position, timing, route
Train
DAS data visualization

Figure 7.1 : DAS tasks done at Traffic Control Centre (TCC)

In figure 7.2, DAS intelligence is shared between TCC and train. TCC computes various critical parameters like previous architecture. DAS definitions and displays are done onboard. The solution optimizes the exchange of information between TCC and onboard in real-time. But, the advice can be poor if the real characteristics of the train system differ significantly from the characteristics known by TCC. The computation should be done correctly where it is easier to access the required data.
In figure 7.3, DAS tasks are mainly onboard. DAS intelligence is implemented in the train. TCC computes a set of functions as mentioned previously. It can adjust speed and optimizes energy to drive the train based on advanced algorithms. The cost of communication between TCC and the train is reduced. But, there is risk of consistency of local optimization.

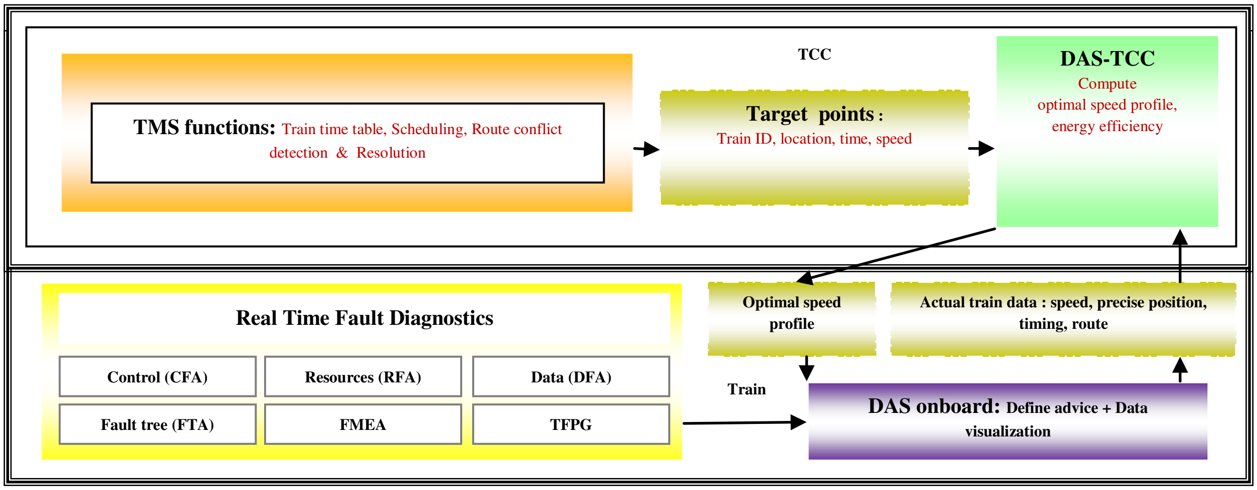

TMS functions: Train time table, Scheduling, Route conflict detection & Resolution
TCC
Target points : Train ID, location, time, speed
DAS-TCC
Compute optimal speed profile, energy efficiency
Real Time Fault Diagnostics
Control (CFA)
Resources (RFA)
Data (DFA)
Fault tree (FTA)
FMEA
TFPG
Optimal speed profile
Actual train data : speed, precise position, timing, route
Train
DAS onboard: Define advice + Data visualization

Figure 7.2: DAS tasks shared between the train and traffic control centre (TCC)

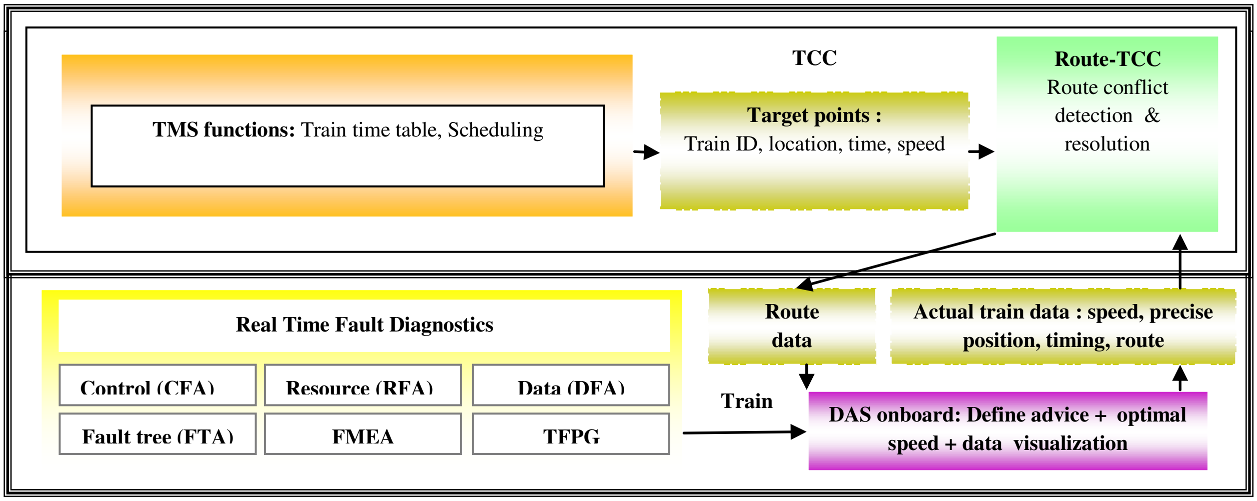

TCC
TMS functions: Train time table, Scheduling
Target points :
Train ID, location, time, speed
Route-TCC
Route conflict detection & resolution
Real Time Fault Diagnostics
Control (CFA)
Resource (RFA)
Data (DFA)
Fault tree (FTA)
FMEA
TFPG
Route data
Actual train data : speed, precise position, timing, route
Train
DAS onboard: Define advice + optimal speed + data visualization

Figure 7.3 : DAS tasks mainly onboard in the train

Computing schema **: This schema performs data processing task with the support of algorithmic intelligence. There may be various options for computing schema such as data processing only at TCC, data processing in a standalone system, data processing integrated with DMI, data processing integrated with third party applications (e.g. communication, position services), data processing integrated with train management system. In case of option 1, the processing takes place at the TCC and DAS only receives advice and displays it to the driver. It involves installation of minimum equipment on the train. Onboard stand-alone system requires a dedicated processing unit at a suitable location of the train. This option requires dedicated space and connections but can be installed through minimum interaction with cab and other onboard systems. Another option is to integrate data processing unit with driver machine interface. It reduces the number of modules to be installed but the maintenance task may be difficult. Another option is to integrate data processing unit with other applications (e.g. positioning, communication) through shared services. The computing schema performs various types of tasks such as tracking train movement, prediction of future train movement, conflicts detection and resolution, finding new target train timings to avoid conflicts and estimation of speed profiles and choice of advice to the driver.**

Networking or communication schema **: This schema controls exchange of data between traffic control centre, trackside and train through various types of communication options such as 3G/GPRS/4G data communication network, with or without integral antenna, 3G/GPRS/4G data to a communications gateway on the train, GSM-R text messaging and ERTMS/ETCS data communications. Another interesting issue communication through SMS between TCC and DAS. In case of 3G/GPRS/4G to DAS with built-in antenna, data communications to moving trains is provided via public telecom providers through GPRS, 3G and 4G by mounting data terminal within DAS equipment on the train with an integral aerial. No external connection is required to DAS but there may be poor communication coverage in several zones and electromagnetic compatibility problems (EMC). In**

case of 3G/GPRS/4G to DAS with external antenna, DAS with integral data terminal is permanently installed on a train. The only external connection is the antenna. The schema of 3G/GPRS/4G to a communications gateway onboard requires the existence of a shared communications server on each train integrated with a shared positioning system. .It is a costly option though it avoids installation of antenna over train roof. These schemes can use dedicated railway GSM-R network and public networks. It is an open agenda whether it is possible to adopt smartphones using 5G / 6G / 7G / 8G wireless communication schema with high speed of data exchange and also Internet of Thing (IoT) for sophisticated driver advice system in future.

Application schema: **A simple DAS may provide predefined timetable information and other generic advice on paper or on a screen. It may be stand alone onboard applications with timetable information and other critical data loaded into the system, independently of the traffic management system. A complex DAS may provide the driver with dynamic advice on how to drive the train as per predefined timetable. The onboard advisory component receives pre-planned timetable, route and train related information from existing traffic management system and computes advice dynamically as per the behaviour of the driver. A sophisticated DAS may provide intelligent advice to the driver of a train based on real time traffic plan. The basic objective of the system is to optimize traffic flow for the railway network by dynamically adjusting the timetable to avoid conflicts. The onboard advisory component is linked to a real-time traffic management system that can calculate new train timings to avoid conflicts and communicate them to the driver.**
One of the key components of DAS is *Driver Machine Interface (DMI)*. **The driver of the running train should be able to see it regularly; it should be positioned in his field of vision on or around the cab desk. There may be various options of DMI such as portable device on the cab desk, dedicated DAS-DMI permanently fitted, integrated with ERTMS/ETCS DMI, integrated with TMS DMI, integrated with GSM-R DMI. DMI system may be implemented in a portable device carried by the driver or it may linked with other parts through wired or wireless link. It incurs minimum hardware cost and it is possible to replace faulty unit easily. But, the portable device may be vulnerable to mismanagement, loss or damage. Another possible option is to permanently modify the dashboard to accept a dedicated display screen for DAS. The screen size and information display can be optimized for the application but there are space constraints. Another important component of DAS is** *train positioning system* **to determine the location of a train in real-time so that DAS can provide correct speed advice. There may be various options of train positioning system such as dedicated GNSS positioning system with or without integrated antenna, shared GNSS positioning system on the train, ERTMS/ETCS positioning system and train positioning with information available from TCC. GNSS with built-in antenna requires a dedicated GNSS positioning system with the support of satellite communication. Alternatively, GNSS can be connected with external antenna on the roof of the train.**

Data schema **: DAS can provide various types of information to the driver of a train such as explicit driving instructions (e.g. current speed target, time series analysis of train speed profile, advice to speed up or slow down), temporal information (e.g. : train running status, time delay optimized speed profile to realize time table), decision support information (e.g. gradient profile, energy usage, position of other trains, conflict, traffic congestion) and a set of monitored performance metrics (e.g. primary and secondary delays, capacity utilization, route conflicts, traffic congestion, signaling errors and real-time train scheduling and time table). One of the critical features of data schema is driver integration through human machine integration: alternative context of advice in terms of 'follow-me' or 'trade-off' method (what information is important to the driver) and alternative forms of advice (how the information is transformed to advice). DAS could guide various parameters such as distance or time interval updated advice, event updated advice, updated speed profile advice and contextual advice without target setting. There may be various forms of advice such as suggested speed based on difference in current speed and target speed, current target speed and duration and target; time keeping based on difference between the actual time at a particular point in the route and the target time, current target departure and arrival time, action on controls (e.g. brake pressure) and energy savings based on speed and time.**

4. SECURITY

Security Analytics

- **Call real time fault diagnostics for infrastructure and rolling stock monitoring through pattern recognition using artificial neural networks and knowledge based expert systems for fault detection and diagnosis.**
    - **Graph Analytics**
    - **Fault Tree Analytics**
    - **FMEA Analytics**
    - **Data logging and event recording analytics**
    - **Event recording and data analytics**
    - **Online health monitoring analytics**
- **Call *threat analytics***
    - **assess risks of single or multiple threats on RailTech; analyze performance, sensitivity, trends, exception and alerts.**
    - **what is corrupted or compromised: agents, communication schema, data schema, application schema, computing schema and RailTech System?**
    - **time: what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
    - **insights: how and why did it occur? do cause-effect analysis.**
    - **recommend : what is the next best action?**
    - **predict : what is the best or worst that can happen?**
- **Verify security intelligence of RailTech / EVs system at levels L1, L2, L3, L4 and L5;**

Level1 [L1 - access control]:

- **authentication, authorization, correct identification, privacy, audit; confidentiality, data integrity, non-repudiation;**
- **private view of data through role based access control**
- **assess the risk of privacy attack;**

Level2 [L2 - computing and communication schema]: fairness, correctness, transparency, accountability, trust, commitment, rationality;
Level3 [L3 - system performance] : robustness, consistency, liveness, reliability, resiliency, deadlock freeness, lack of synchronization, safety and reachability;
Level4 [L4 - malicious attacks] : detect the occurrence of any malicious attack on the RailTech system.

- **rail network delay due to coremelt or network traffic congestion**
- **rushing attack**
- **sybil attack**
- **false data injection attack**
- **other attacks: data integrity attack, node deletion, flaws in workflows, poor QoS, information leakage, physical attacks on the drivers by terrorists or malicious agents.**

Level5 [L5 - Business intelligence]: audit flaws in payment function computation.

Dr. Simon Rodrigues and Prof. R. Prakash are discussing on the security intelligence of emerging logistics technologies. It is essential to design electrical / hybrid vehicles in terms of security at various levels – L_1, L_2, L_3, L_4 and L_5. Level L_1 verifies system performance in terms of safety, reliability, consistency, stability, robustness and reach. The other critical design issues are also associated with resiliency, reachability, deadlock-freeness, synchronization and interactive intelligent communication among electrical / hybrid vehicles. Solid-state battery technology has higher energy density and tolerance to higher temperatures; may avoid the use of dangerous toxic materials, nonflammable and safer; can withstand higher voltage and longer life-cycle and support faster recharging rate. The safety of electrical / hybrid vehicles depends on access control at level L_2 in terms of authentication, authorization of the drivers, correct identification of the system components and audit of quality control issues. The security schema is also designed and verified at level L_3 in terms of fairness, correctness, transparency, accountability, trust and commitment. The safety of the electrical / hybrid vehicles may be threatened at level L_4 through the corruption of various stakeholders such as car manufacturers, drivers, passengers and battery charging station supervisors. The design of the vehicles is expected to assess and mitigate the risks of various types of attacks at level L_5 such as false data injection, sybil, shilling and traffic congestion.

***Vehicle to Vehicle (V2V) Communication* for Anti-collision System : The scope of emerging communication technology has been explored for intelligent V2V communication against the threats of accidents and collisions of vehicles on roads. The wireless technology is going through an evolution of a set of generations (1G→2G→3G→4G→5G→G→7G). One of the most interesting applications of this emerging technology is Vehicle-to-Vehicle (V2V) communication, Most cars are**

expected to have a 4G or 5G cellular connection for V2V communication and the security of the drivers and passengers. 5G Automotive Association have been promoting C-V2X communication technology. It provides for communication between vehicles and communication between vehicles and infrastructures, leading to increase in autonomous self-driving cars and IOT (Internet of Things). The speed of 5G technology in upcoming self-driving cars may be vital in helping the capabilities of autonomous cars realize their full potential (Llanasas, 2019). Current 4G network doesn't possess the required speed needed to provide self-driving vehicles that could prevent catastrophic accidents or collision (Llanasas, 2019. 5G is expected to be the basic building block of anti collision system of next generation vehicles.

5G is the fifth generation wireless technology for digital cellular networks with wide deployment in 2019. The frequency spectrum of 5G is classified as millimeter waves, mid band and low band. Low band uses a similar frequency range as 4G. 5G millimeter wave is the fastest having actual speeds 1–2 Gbit/s down. Frequencies are above 24 GHz reaching up to 72 GHz, above lower boundary of extremely high frequency band. 5G mid-band is the most widely deployed in over 20 networks; speed in a 100 MHz wide band is 100–400 Mbit/s down. 5G low-band offers similar capacity to advanced 4G; latencies between 25 -35 milliseconds. 5G networks are digital cellular networks in which the covered service area is divided into *cells*. Analog signals (e.g. sounds, images) are digitized by an analog-to-digital converter and transmitted as a stream of bits. All 5G wireless devices in a cell communicate by radio waves with a local antenna array and low power automated transceiver in the cell, The local antennas are connected with telephone network and Internet through a high bandwidth optical fiber or wireless backhaul connection. A mobile device crossing from one cell to another is automatically handed off seamlessly to the new cell.

6G (sixth generation) is the successor to 5G cellular technology; 6G networks are expected to use higher frequencies, higher capacity and much lower latency than 5G networks. 6G is a wireless technology that is beyond 5G. China has officially launched R&D works for 6G mobile networks. It would be about a decade before 6G comes along, NTTDoCoMo has presented the evolution of wireless technology from 3G in 2000s, 4G in 2010, 5G in 2020 and it is reasonable to expect 6G in 2030. It is not exactly known how fast 6G will be yet. It may be governed by the standards of International Telecommunication Union (ITU). If everything connects together using 5G, 6G with higher data speeds and lower latency makes instant device-to-device connection possible in various application such as autonomous cars, drones and smart cities, integration of our brains with computers and greatly improved touch control systems. 7G is the next generation communication technology. It is being adopted in Norway, China, Japan and other developed countries of the world. In Norway, Internet speed is fastest. Utilizing superior design and technology, 7G Network is expected to deliver millions of calls reliably every day,

The air interface defined by 3GPP for 5G is known as New Radio (NR), and the specification is subdivided into two frequency bands, FR1 (below 6 GHz) and FR2 (mmWave) each with different capabilities. The next issue is frequency range 1 (< 6 GHz); maximum channel bandwidth defined for FR1 is 100 MHz, the most widely

band is around 3.5 GHz. For frequency range 2 (> 24 GHz), minimum channel bandwidth defined for FR2 is 50 MHz and the maximum is 400 MHz, From the perspective of *performance analysis;* 5G speeds are expected to range from ~50Mbit/s to over 2Gbit/s even 100Gbit/s, 100x faster than 4G. The fastest 5G, known as mmWave, delivers speeds of up to and over 2Gbit/s. The latency of 5G is 8–12 milliseconds. It is governed by International Telecommunication Union's IMT-2020 standards.

Next, let us consider the deployment of 5G, Nine companies sell 5G radio hardware and 5G systems for carriers- Altiostar, Cisco Systems, Datang Telecom, Ericsson, Huawei, Nokia, Qualcomm, Samsung and ZTE. Large quantities of new radio spectrum (5G NR frequency bands) have been allocated to 5G. 5G devices include Samsung Galaxy S10 5G. The technology is expected to be available in Australia, Argentina, Bulgaria, Canada, China, Finland, Germany, India, Monaco, Netherlands, New Zealand, Norway, Pakistan, Philippines, Romania, Russian Federation, San Marino, South Africa, South Korea, Taiwan, Thailand, Uruguay, Vietnam, Qatar, Mexico, USA, Sweden and Panama.

ITU-R has defined three main uses for 5G as faster and reliable connection - Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). Only eMBB is deployed in 2019; URLLC and mMTC are several years away in most locations. eMBB uses 5G as a progression from 4G with faster connections, higher throughput, and more capacity; mMTC is expected to connect a large number of low power, low cost devices, which have high scalability and increased battery lifetime, in a wide area. 5G technology may connect some of 50 billion connected IoT devices. So far, we have discussed the strength of the emerging wireless technologies. But, there are various constraints such as interference, security, surveillance and health concerns. The spectrum used by remote sensing, weather and Earth observation satellites will potentially be significant without effective controls. The technology has health concerns; the radiation could have adverse health effects. There are concerns of data security and privacy, surveillance concerns, threats of potential espionage of foreign users by 5G equipment vendors.

***Internet of Things (IoT)* : Internet of Things is the integration of several technologies and communications solutions such as identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols shared with next generation Internet and distributed intelligence for smart objects fitted with EVs / HVs. IoT can be effectively used for assisted driving, transportation and logistics domain. Advanced cars, trains, buses, bicycles, roads and transported goods are becoming equipped with sensors, RFID tags, actuators and processing power. These objects can send important information to traffic control sites for better transportation planning, effective route optimization for energy saving, tracking of delivery time and delay, faults and monitoring in the supply chain and transportation network. These objects can provide important information to the driver and/or passengers of a car to allow better navigation, safety, collision avoidance systems and monitoring of transportation of hazardous materials.**

Real-Time Fault Diagnostics (RTFD) **: The fourth element of deep analytics is security. Please refer to five test cases as discussed in section 9. We have analyzed those cases and outline the aforesaid security schema comprehensively. It is essential to monitor and detect faults of a complex real-time system; assess the chance of various types of faults and explore efficient and reliable fault detection and isolation methods based on artificial intelligence [30]. The basic building blocks of real-time fault diagnostics are soft computing and AI methods such as knowledge based expert system, model based system, if-then rule based system, artificial neural network (ANN), fuzzy logic, genetic algorithm (GA), decision tree and Bayesian network. It is possible to monitor real-time system, faults detection, diagnosis and correction at process and functional levels through a set of quantitative and qualititative performance metrics.**

Faults may occur due to various reasons such as failure of hardware components (e.g. sensors, triggers), environmental factors (e.g. noise) and flaws in software (e.g. algorithms, logic, coding, protocols, invalid and incorrect inputs and feedback, knowledge base, inference mechanism and knowledge representation). There are other constraints such as inconsistency in knowledge base and flaws in knowledge engineering, learning errors and data visualization. Traditionally, track geometry is monitored using accelerometers and camera; cracks in tracks are detected through non-destructive test; measurements are acquired through various sensors of specialist trains and data is analyzed on the train. If the value is above predetermined threshold, then it requires the effort of the experts to identify and diagnose the faults.

Real-time fault diagnostics are basically condition monitoring systems having three core components: (a) data logging and event recording system, (b) event recording and data analytics and (c) online health monitoring system. The first component can detect faults (e.g. change in logic and operation time), can give hard evidence of accidents and other abnormal conditions caused by the malfunctioning of RailTech system and also can record the performance and status of critical equipments and operations in the form of digital data. On-Train Maintenance Recorder (OTMR) is equivalent to a black box and may use GPS and other sophisticated systems for real time data communication.

The second component may have intelligent data analytics (e.g. statistical analysis, sequence mining) and remote access to critical data. The second component may record door opening time, traction current and energy usage. Track based monitoring is useful for the verification of the performance of vehicles such as monitoring of wheel with strain gauge or fibre optic sensors and the monitoring of hot axles boxes.

The third component is basically knowledge based expert system which can collect digital and analog data from various critical equipments, analyze sensed data, compare with an inbuilt database of healthy and simulated faulty operational modes, flag alarms and recommend diagnosis to the drivers and maintenance workforce. Automated system verification is essential for scalability and robustness in fault diagnosis. The basic building blocks of RTFD are following three analytics the output of the same is fed to DAS.

Graphical Analytics [GA]

Call Graphical Analytics; Verify robustness and consistency of RailTech system performance;

- **Time : Sense failure propagation in dynamic systems through [TFPG = F, D, E, M, ET, EM, DC, DS]; [TFPG]**
  - **TFPG transition system : S = (X,I,T); X= state variable, I - initial state, T - state transition;**
  - **F : failure nodes;**
  - **D : discrepancy nodes;**
  - **E : edges connecting all nodes;**
  - **M : system modes;**
  - **ET: E, a map that associates every edge with minimum and maximum time for the failure of propagation;**
  - **EM: E, a map that associates every edge with a set of modes either ON or OFF;**
  - **DC: D, a map defining the class of each discrepancy either AND or OR;**
  - **DS: D, a map defining monitoring status of discrepancy as either M (when discrepancy is monitored by alarm) or U (when the discrepancy is not monitored).**
- **Control flow [Control Flow Analytics (CFA)]**
- **Resources flow [Resources Flow Analytics (RFA)]**
- **Data flow [Data Flow Analytics (DFA)]**

Detect, isolate and correct problems early and re-allocate resources as per demand.
Output :

- **Timed Failure Propagation Graph (TFPG)**
- **System performance scorecard**
- **Data visualization : error trail / error trace / fault propagation path**

The graphical analytics (GA) analyze RailTech System performance from the perspectives of four dimensions: time, control flow, resources flow and data flow. TFPG considers only time failure but ignores the other important aspects of vehicle diagnostics such as control, resources and data flows. RTFD is expected to give a comprehensive view of system failure not only in terms of time delay but also flaws in control, data and resource flows. It is an interesting research agenda whether a single graph can show the propagation of different types of failures in system performance from the perspectives of time delay and flaws in resource, data and control flows simultaneously and comprehensively.

***Time Failure Propagation Graph* (TFPG) : Timed Failure Propagation Graph is a rich formalism and is used to model the occurrence and propagation of failure and their direct and indirect effects, Boolean combinations of faults, time delays, events and state transitions in the design of real-time fault diagnostics of a complex, autonomous and dynamic system. There are several important issues: no critical**

state of a system should be ignored; no spurious and nonexistent sate should be considered for analysis; it is essential to perform fault detection, isolation and recovery, sense and compute time delays between events correctly and validate completeness and tightness of the graph through intelligent model checking algorithms. TFPG can model and reason the issues of spurious and missing alarms, intermittent faults and reduction of a large scale vehicle diagnostics system. It is an interesting open research agenda whether TFPG can verify performance of RailTech system in terms of reliability, consistency, liveness, safety, robustness, stability, deadlock freeness and reachability comprehensively.

Timed Failure Propagation Graph is a directed graph model (Figure 7.4); the structure has a set of nodes (V) and edges (E). The nodes represent failure modes (F) i.e. root events of the propagations of failure and discrepancies (D) i.e. possible deviations from nominal behavior caused by failure modes. Failure modes do not have any incoming edges; discrepancies must have at least one incoming edge and must be reachable from a failure mode node. Circular paths are possible. Edges (E) model the dependency between the nodes (V = F∪D) and capture propagation of time delays; the edges can be activated or deactivated based on a set of operation modes (M). ET is a map that associates every edge with minimum and maximum propagation time (t_{min},t_{max}) of a failure. EM is a map that associates every edge with a set of modes in M. DC: D is a map defining the type of each discrepancy either AND or OR.

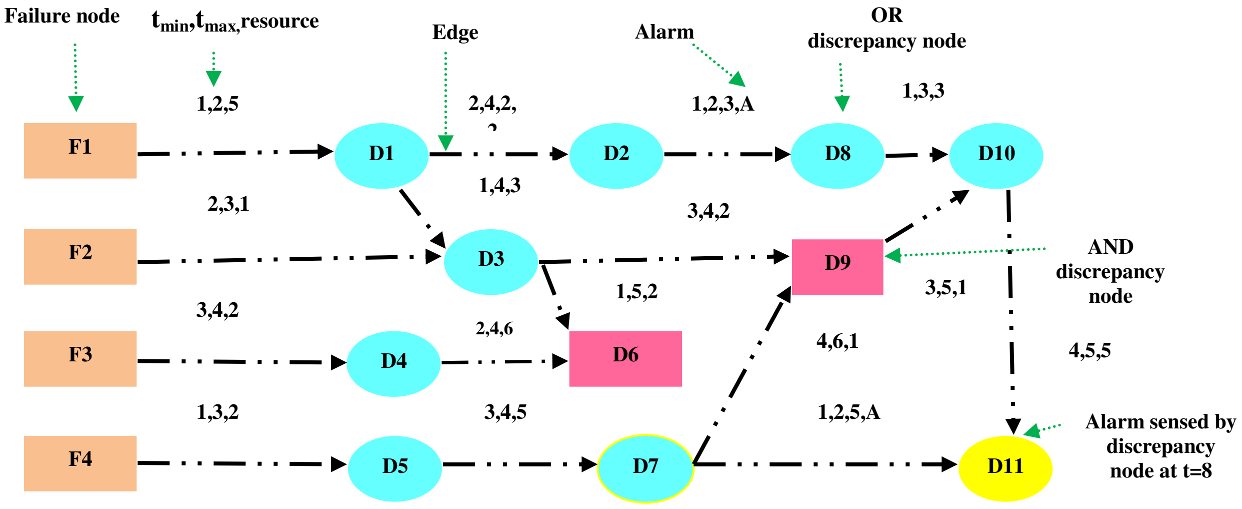


Figure 7.4: Time Failure Propagation Graph

Is there any other type discrepancy apart from AND or OR such as NAND, NOR, NOT, XOR and loop? Section 5.1.1.2 gives an overview of various types of control flow patterns in RailTech system. DS: D is a map defining monitoring status of discrepancy as either M when (discrepancy is monitored by alarm) or U (when the discrepancy is not monitored). A TFPG transition system is represented by S = (X,I,T) where X is a set of state variables; I(X) is initial state, X' is next state of X and T represents transition relation. A state s of S is an assignment to the state

variable of X. A trace of s is an sequence λ := $s_0,s_1,...s_n$ such that s_o = I(X) and (s_i,s_{i+1}) = T(X,X').

Control Flow Analytics [CFA]
System : RailTech system (Mechanical, Electrical, Electronics, Information system : Driver Advice System [DAS], Communication system);
Assess risks: Verify correctness, reliability, consistency, liveness, deadlock freeness, synchronization and reachability in control flows.

- **Basic control flows : Sequential, Parallel split, Synchronization, Exclusive choice, Simple merge;**
- **Special branching and synchronization control flows: Multi choice, Synchronizing merge, Multi merge, Discriminator, m-out-of-n join;**
- **Structural control flows : Loop, Implicit or explicit termination, Multiple instances;**
- **State based control flows: Deferred choices, Interleaved parallel routing, Milestone, Cancel;**

Mitigate risks.

- **Replace faulty components through proactive and reactive maintenance;**
- **Rectify circuit connectivity;**
- **Correct Boolean logic in electrical and electronic circuit: AND / NAND/ Exclusive OR/ NOR/ XOR/ XNOR/ NOT;**

Resource Flow Analytics [RFA]

System: RailTech system (Mechanical, Electrical, Electronics, Information and Communication system), smart coaches;
Assess risks: Verify correctness, and fairness of resource management;

- **Resource planning: sense demand supply mismatch.**
- **Resource allocation : automatic / semi-automatic execution, direct allocation, role based allocation, deferred allocation, authorization in allocation, separation of duties, case / exception handling, capability based allocation, history based allocation, organizational allocation, resource initiated allocation**
- **Resource distribution : Single / multiple resources distribution, early / late distribution, priority queue, autonomous resource allocation;**
- **Resource mobilization**
- **Resource sharing**
- **Resource delegation, escalation, deallocation, suspension, resumption, skip, redo, stateful / stateless reallocation, simultaneous / chained execution;**

Mitigate risks:

- **Optimal resource allocation (e.g. avoid shortage or surplus of resources such as fuel, safety stock)**
- **Sensor based on board condition monitoring system**

    - Monitor health of critical system components (e.g. wheels) through sensors, CCTVs, smoke detectors, Fire extinguishers, IoT and integrated information system.
    - Real-time fault detection: Detect defects and major causes for derailments and delays and deterioration in tracks, running trains and other rail infrastructure.
    - Trade-off cost vs. comforts / luxury;

Data Flow Analytics [DFA]

System : RailTech system (Information and Communication schema of DAS)
Data elements: Single / multiple instance DAS operating environment data, Atomic and block task data, Boolean and numeric data, time series data;
Assess risks. Verify correctness, reliability and consistency of data schema.

- **Data visibility**
- **Data interaction among various elements of DAS**
- **Data transfer between various components of networking, computing and application schema of DAS**
- **Data transformation**
- **Data based routing of various control flow patterns associated with DAS**
- **Data analysis / mining**
    - **ETL (Extract, Transform, Load) mechanism**
    - **Data cleaning and selection**
    - **Knowledge discovery from data**
    - **Data visualization**

Mitigate risks:

- **Sense flaws in data flow, streamline data management.**
- **Detect noise, missing, imprecise sensor data; clean data before analysis.**

Fault Tree Analytics [FTA]

Call fault tree analytics;
Objectives : identification and analysis of conditions and factors that cause the occurrence of faults;
System verification mechanism : verify reliability and safety of RailTech system performance through top-bottom approach;

- **Define fault tree structure based on system data, scope and applications related to RailTech System;**
- **Fault tree development, construction and evaluation;**
    - **Events**
        - **Basic event /* failure of a component */**
        - **External event /* normally expected to occur */**
        - **Undeveloped event /* insufficient data */**
        - **Conditioning event /* conditions that control logic gates */**
    - **Logic gates**
        - **AND gate /* o/p will occur only if all independent i/ps occur */.**

        - **Priority AND gate /* o/p occurs if the i/ps occur in a specific sequence specified by a conditioning event */**
        - **OR gate /* the o/p will occur if any i/p occurs */**
        - **Exclusive OR gate /* o/p will occur if exactly one i/p occurs */**
        - **Inhibit gate /* o/p will occur if i/p occurs under an enabling condition specified by a conditioning event*/**
- **Compute failure rate from fault tree analysis;**

Output: FTA provides following output to the driver through automated data visualization tool.

- **report**
- **error trail / error trace / fault propagation path**

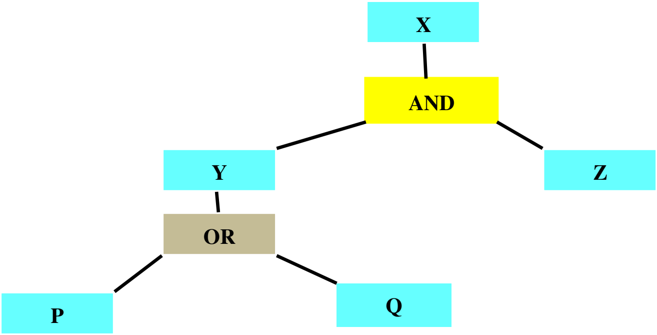


Figure 7.5: Fault tree

FTA is generally used as a diagnostic tool to understand the logic leading to a faulty state; does root cause and pareto analysis; evaluates, monitors and controls safety, consistency and reliability of a complex system. FTA is a deductive reasoning that analyses an undesired top level event and identifies fault configurations i.e. minimal cut sets; a cut set is a set of faults that represents a necessary, but not sufficient, condition that may cause an undesired state of a system. Event X occurs only if both events Y and Z occur. Event Y occurs if either event P or Q occurs. The standards, frequently used symbols, conventions, events and logic gates for fault tree diagrams can be found in .

Failure Mode Effect Analytics [FMEA]

Call Failure Mode Effect Analytics (FMEA);
Objectives : identification and analysis of conditions and factors that cause the occurrence of faults;
Verify reliability and safety of RailTech system performance through bottom-up approach;
Output:

- **FMEA Table: it highlights causality relationship between faults and undesired states or properties.**
- **Data visualization -error trail / error trace / fault propagation path;**

Let us exercise a comparative analysis on TFPG, FTA and FMEA. FTA is a deductive and top-down method which analyzes the effects of a fault and events on a complex system. FMEA is an inductive and bottom-up method which analyzes the effects of a single component on a system. FTA shows how a system is protected to single or multiple faults. It is not good at finding all possible faults of a system. FMEA is good at finding all possible faults exhaustively and their local effects. It is not good at finding multiple failures and their effects at a system level. FTA considers external events but FMEA does not consider it. TFPG allows fine grained and precise analyses that FMEA cannot do. FTA explores only subsets of propagation paths in response to specific events, TFPG presents a more comprehensive and integrated view of failure in a complex and dynamic system.

Knowledge based Expert System

Abnormal operating conditions and faults may cost rail system significantly but may be prevented through intelligent prediction and control mechanism of knowledge based expert system. An expert system is expected to monitor, detect and diagnose abnormal conditions of rail system and provides safeguards against unexpected process conditions. It is possible to model faults and instability in a complex rail system through expert system which is basically a knowledge based real-time fault diagnostics. The expert system uses the valuable knowledge from the experts, operators and real-time data from various sensors, measuring instruments and various electrical and electronic devices connected to the rail system. Soft computing algorithms (e.g. fuzzy logic and ANN) may be used for mining acquired real-time data and knowledge discovery from data.

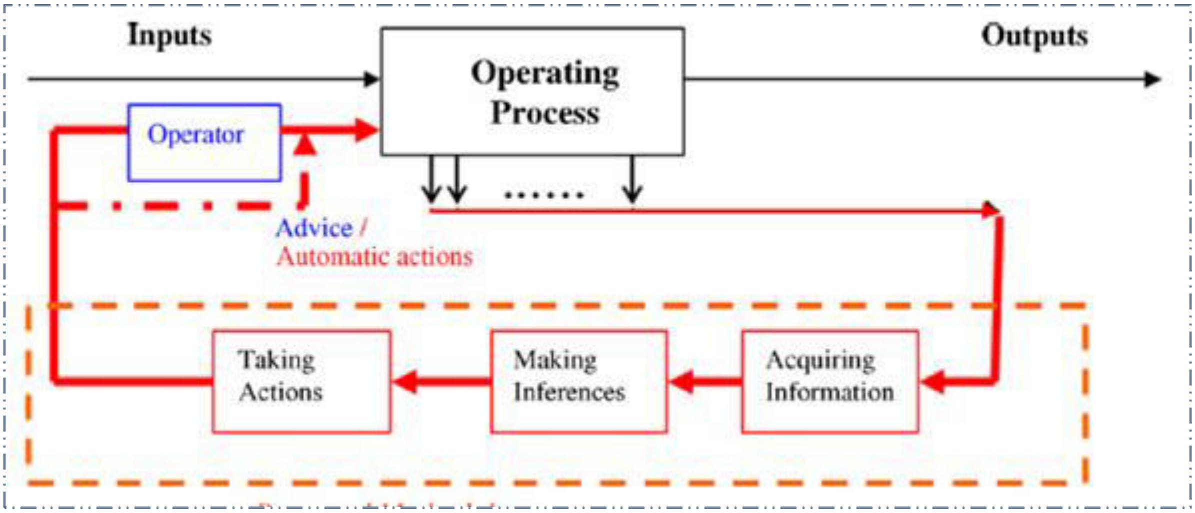


Figure 7.6 : Knowledge based expert system for real-time fault diagonistics

There are two methods of fault diagnosis : model based approach and knowledge based approach. Model based approach adopts quantitative models to estimate states and parameters of a system. But, it is almost impossible to obtain a model that exactly matches the process behavior of rail system in practice. The mismatch between the behavior of the model and rail system may lead to large error signals.

Abnormal operation may cause false alarms unless appropriate thresholds are used. It may be impossible to model non-linear systems by analytical equations. These negative aspects demand the support of alternative knowledge based methods in fault diagnosis such as ANN, fuzzy logic and CBR. Knowledge based fault diagnosis is done based on the evaluation of real-time data according to a set of rules which human experts (e.g. train drivers, engineers, support staff) have learnt from past experience. The knowledge may be input and output process variables, patterns of abnormal process conditions, fault symptoms, Linear approximation of nonlinear system may result significant errors. The combined approach of knowledge based fault diagnosis with real-time process variables improves the reliability, consistency and efficiency of the system. Knowledge based fault diagnosis has three basic steps [Figure 7.6]: (a) acquire real time process data from sensors and intelligent mechanical, electrical and electronic devices; the sensed variables indicate problem of safety and stability of rail system; (b) make inferences or diagnosis based on acquired process data; (c) take actions based on inferences such as raising alarms, informing drivers and automated on/off operation of connected equipments for resiliency of the system.

Rail system demands continuous monitoring through an adaptive security schema. Advanced analytics is the basic building block of next generation security protection which should be able to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. User Entity Behavior Analytics detect anomalous patterns by comparing with the normal profile and the activities of the users and trigger alarms by sensing single or multiple attacks on rail system. Dynamic data protection is an effective way to move towards adaptive security architecture. DDP surfaces anomalies and adjusts individualized data security controls proactively in near real-time to protect critical data of rail system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security schema Adaptive security is a critical feature of a technology that monitors rail network in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of rail system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks.

5. STRATEGY

Strategy Analytics

***Agents*: System analysts, business analysts, scientist, engineers, technology management consultants;**

***Strategic moves* : Focus on emerging logistics technologies.**

- **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements – scope, system, structure, security, strategy, staff-resources, skill-style-support;**
- **Define a set of security goals and emerging technologies accordingly.**

- ✪ Do SWOT analysis: strength, weakness, opportunities and threats of existing technologies as compared to emerging technologies.
  - Fair and rational business model innovation.
  - Who are the consumers?
  - What should be the offering of products and services?
  - What do the consumers value?
  - What is the rational revenue stream ?
  - How to deliver values to the consumers at rational cost?
- ✪ Do technology life-cycle analysis on 'S' curve : presently at emergence phase of 'S' curve.
- ✪ Explore technology innovation-adoption-diffusion strategy.
  - Real-time fault diagnostics using fault tree analytics, FMEA and TFPG.
  - Automated verification of security intelligence at multiple levels using deep analytics
  - Distribution of intelligence
  - Processing unit integration
  - Integration of driver's interfaces, train positioning and communication schema
  - Exchange of information between track and train
  - SWOT and TLC analysis
- ✪ Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.
- ✪ Adopt '4E' approach for innovation projects on logistics technologies : envision, explore, exercise and extend.

Prof. Prakash is analyzing the strategic moves for the innovation, adoption and diffusion of emerging logistics technologies. This element should be analyzed from different perspectives such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovation is closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of the technology of electrical and hybrid vehicles through logical and analytical reasoning.

The technological innovation is closely associated with R&D policy and organizational learning strategies in new product development and process innovation. There are various strategies of learning such as learning by doing and learning before doing. Learning by doing is effective in those technologies which demand low level of theoretical and practical knowledge. On the other side, learning before doing is possible through various methods such as prototype testing, computer simulations, pilot production run and laboratory experiments. It is effective for the innovation of EVs where deep practical and theoretical knowledge

can be achieved through laboratory experiments that model future commercial production experience.

Let us explore the role of deep analytics on technological innovation of EVs. It is interesting to analyze the impact of different learning strategies and timing of technology transfer on product development performance, process re-engineering and R&D cost of this technological innovation. It is important to compare the effectiveness of various types of learning strategies in terms of cost, quality and time. It is also critical to analyze the relationship between process innovation and learning curve in terms of dynamic cost reduction and improvements in yield. It is essential to identify the critical success factors (e.g. resource allocation, ERP and SCM strategies) that influence the rate of learning and superior performance.

It is rational to evaluate strength, weakness, opportunities and threats of the technological innovation on electrical and hybrid vehicles. There may be major and minor strengths and weaknesses. Strength indicates positive aspects, benefits and advantages of EVs. Weakness indicates negative aspects, limitations and disadvantages of the technology. Opportunities indicate the areas of growth of the market of EVs and industries from the perspective of profit. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses.

Let us first do SWOT analysis on EV technology and explain the strength of EVs. Wide spread adoption of electrical and hybrid vehicles can limit the environmental pollution of conventional fuel based transportation and can reduce dependence on oil (e.g. petrol and diesel). Intelligent supply chain contracts and switching stations may increase driving. The adoption of electrical vehicles is safe, reliable and consistent. Rational policy intervention is expected to consider battery purchase subsidies and R&D for advancement of battery techniques in terms of safety, system performance, cost, life-span, specific energy and specific power. Sustainable green transportation is a critical research agenda of government, environmentalists, industry and academics; green fuel (electrical, biofuel, hydrogen, natural gas) can limit environmental pollution and oil dependence.

Next, let us talk about the weakness of EV technology. The transition from conventional gasoline vehicles to EVs poses several challenges. Increase in adoption of EVs may create unprecedented strains on the existing power generation, transmission and distribution infrastructure. Renewable energy is typically intermittent which may result a potential mismatch between supply and demand. There are other constraints such as range anxiety and high battery cost that may limit consumer adoption. It is rational to adopt novel switching station based solution. Electrical and hybrid vehicles can use standardized batteries that when depleted can be switched for fully charged batteries at switching station. The consumers can pay for miles driven and don't pay for upfront battery purchase. In case of range anxiety, an EV may have insufficient range to reach its destination. It demands technological advancement and high energy storage capacity of batteries.

Next, let us explore the opportunities and threats of EV technology. Transportation sector is a significant contribution to environmental pollution. Geopolitical uncertainties often result increased vulnerabilities of oil based transportation infrastructure. The adoption of electrical vehicles is expected to result the growth of

electrical drives, hybrid vehicles, renewable energy (e.g. solar microgrid, wind, tidel), power plants, standardized batteries and electrical battery charging stations. This business model requires an efficient payment function and market clearing mechanism. It is not rational to buy batteries; rather it should be replenished at battery charging stations. EVs require adequate supply of electrical energy; thermal power may not be an interesting option from the perspectives of environmental pollution.

SWOT analysis on Smart Batteries **: Let us exercise SWOT analysis on Li-ion and solid state batteries. Electrical vehicles may be dearer to buy but cheaper to run. But there are issues of range and rate of efficient battery charging mechanism. Electrical batteries may be the game changer in the innovation of electrical and hybrid vehicles technology. Solid state batteries replace the wet electrolyte of lithium ion batteries with a solid electrolyte. Current lithium-ion batteries are flammable and produce heat and have short life span; constant charging and discharging slowly erodes the performance of the battery. Smart batteries are expected to be simple in design, cheaper and lighter in weight as compared to present Li-ion batteries; won't need liquid cooling; the smart batteries should be long lasting, fire-proof and should permit faster charging.**

Let us discuss the limitations of existing battery technologies of EVs. SSBs are generally very expensive; those batteries have other limitations such as poor system performance at low temperature, impact of pressure, breakage due to mechanical stress and risks of dendrites. Li metal dendrites from the anode piercing through the separator and growing towards the cathode in the form of crystal like structure. Generally, solid Li anodes in SSBs replace graphite anodes in Li-ion batteries for higher energy densities, safety, and faster recharging time. Solid Li anode experiences the formation of Li dendrites due to the reactivity of the metal. Li dendrites penetrate the separator between the anode and cathode to prevent short circuits. The penetration of Li dendrites into the separator may cause short circuit, overheating, fire or explosion from thermal runaway propagation and reduction of columbic.

There are also financial barriers of existing battery manufacturing plant; they have to invest significantly on solid state batteries. There is a huge difference between a technology that works on a small scale and one that is ready for mass market production. Cars charge as they drive; EVs demand the support of smart batteries which should be cheaper, smaller in size, light weight, non-flammable, increased life cycle (say 2-10 years), higher capacity and fit for faster charging and long range. The industry is looking for a sustainable, affordable and widespread energy conversion system. Is it possible to have a battery with two times the density of current batteries at 1/5 of the cost?

Technological life-cycle analysis **: Deep analytics can evaluate and explore the technological innovation of EVs in terms of technology life-cycle, technology trajectory, S-curve, technology diffusion and dominant design. No element in this universe exists eternally. Similarly, the technology of EVs has emerged and is now growing to some level of maturity It is essential to evaluate the status of each**

technological innovation through TLC analysis. Some technologies may have relatively long technology life-cycle; others never reach a maturity stage. Emergence of new technologies follows a complex nonlinear process. It is hard to understand how the technology life-cycle interacts with other technologies, systems, cultures, enterprise activities and impacts on society. All technologies evolve from their parents at birth or emergence phase; they interact with each other to form complex technological ecologies. The parents add their technological DNA which interacts to form the new development. A new technological development must be nurtured; many technologies perish before they are embedded in their environments. Next phase is growth; if a technology survives its early phases, it adapts and forwards to its intended environment with the emergence of competitors. This is a question of struggle for existence and survival for the fittest. Next phase is a stable maturity state with a set of incremental changes. At some point, all technologies reach a point of unstable maturity i.e. a strategic inflection point. The final stage is decline and phase out or expire; existing technologies of oil fuelled vehicles will eventually decline and are phased out or expire at a substantial cost.

Let us consider the analysis of the performance of a new technology vs. effort; it is basically an S-curve. Initially, it is difficult and costly to improve the performance of the new technology of EVs. The performance is expected to improve with better understanding of the fundamental principles and system architecture. Next, let us analyze the adoption of the technology over time which is also an S curve. Initially, the new technology of electrical and hybrid vehicles may be costly for the adopters due to various uncertainties and risks. Gradually, this new technology is expected to be adopted by large segments of the market due to reduced cost and risks.

The rate of improvement of the new technology may be faster than the rate of market demand over time; the market share increases with high performance. Technological change follows a cyclical pattern. The evolution of the new technology of EVs is passing through a phase of turbulence and uncertainty; various stakeholders of the supply chain are exploring different competing design options of the new technology and a dominant design is expected to emerge alongwith a consensus and convergence of structure. Then, the producers will try to improve the efficiency and design of the EVs based on stable benchmark of the industry. The dominant design of EVs must consider an optimal set of most advanced technological features such as smart batteries, solar power enabled battery charging mechanism and V2V communication, which meet the demand of the customer, supply and design chain in the best possible way.

Technology trajectory **is the path that the technology of EVs takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. It is really interesting to analyze the impact of various factors and patterns of technology trajectories of this innovation today. How to manage the evolution of this technological innovation? The nature of innovation shifts markedly after a dominant design emerges. The pace of performance improvement utilizing a particular technological approach is expected to follow an S-curve pattern. The evolution of innovation is determined by intersecting trajectories of performance demanded in the market vs. performance supplied by technologies. Technology diffusion indicates how new technologies**

spread through a population of potential adopters. It is controlled by characteristics of innovation, characteristics of social environment and characteristics of the adopters such as innovators, early adopters, early majority, late majority and laggards. What should be the innovation model for effective innovation, adoption and diffusion of emerging technology of EVs / HVs? It is rational to adopt K-A-B-C-D-E-T-F model.

It is expected that RailTech will go through emergence, diffusion, development and maturity phases in this decade. At present, the technology is at growth phase of TLC. It is not a trivial task to evaluate and explore technology life-cycle in terms of S-curve, trajectory, diffusion strategy and dominant design of RailTech. It is hard to understand how RailTech interacts with other technologies, systems, cultures, enterprise activities and impacts on society. What should be the innovation model for effective innovation, adoption and diffusion of emerging technology of Railtech security? It is an interesting option to adopt K-A-B-C-D-E-T-F model. Initially, it may be difficult and costly to improve the performance of the RailTech; the performance is expected to improve with better understanding of the fundamental principles and system architecture. The evolution of this technology passes through a phase of turbulence and uncertainty; various stakeholders associated with the system may explore different competing design options of the new technology and a dominant design will emerge through consensus and convergence of structure.

6. STAFF-RESOURCES

Staff-resources analytics

- ***Innovators*** **: R&D units of automobile manufacturing companies; technology management departments of academic institutes, collaborative networks;**
- **Organizational creativity, organization structure, cooperative work culture, human capital management, talent management, knowledge management;**
- **do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.**
  - ✪ ***Man*** **: human capital management (scientists, business analysts, system analysts, project managers, engineers): talent acquisition, talent retention, training, reward and recognition;**
  - ✪ ***Machine*** **(mechanical, electrical, electronics);**
  - ✪ ***Material*** **(steel, paint);**
  - ✪ ***Method*** **: process innovation;**
  - ✪ ***Money*** **: (optimal fund allocation, project management, resource allocation, resource distribution).**

Dr. Rodrigues and Prof. Parakash are presenting on '*staff-resources' for logistics security.* . The sources of EVs innovation may be R&D units of automobiles manufacturing companies, mechanical, electrical and electronics departments of engineering institutes, technology management of management institutes and collaborative networks. Creativity is the underlying process for EV technology innovation which can promote new ideas through shared vision, intellectual

abilities, thinking style, knowledge, personality, motivation, commitment, confidence and group dynamics. It demands the motivation and commitment of the creative people to look at the problems in unconventional ways. Organizational creativity is closely associated with human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routine and incentive policy.

Prof. Prakash is outlining sixth element of deep analytics i.e. staff-resources in terms of 5M – man, machine, material, method and money. 'Man' analyzes various aspects of human capital management of this technological innovation such as talent acquisition and retention strategy, training, payment function, compensation, reward, incentive and performance evaluation. 'Machine' analyzes the basic aspects of tools and automated / semi-automated / manual machines; 'material' analyzes planning of raw materials, equipments, semi-finished and finished goods. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure. Finally, 'money' highlights optimal fund allocation for R&D, rational investment analytics, intelligent project analytics and portfolio rationalization.

It is crucial to analyze the dynamics of technological innovation in terms of sources of innovation and roles of individuals, firms, organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion such as 5M i.e. man, machine, material, method and money; dominant design factors, effects of timing and mode of entry. This innovation demands the commitment of creative people. Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. Some users or customers may innovate based on their own needs. Many firms have set up excellent R&D lab and also collaborative networks with customers, suppliers, academic institutes, competitors, government laboratories and nonprofit organizations. Many universities have defined mission and vision of research on EVs and are contributing through publication of research papers. The Governments of many developed and developing countries are also playing active roles in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators).

A complex technological innovation like EVs often needs collaborative intelligence to manage the gap between demand and supply of a specific set of capabilities, skills and resources. It is possible to control cost, speed and competencies of the technological innovation on EVs through efficient sharing mechanisms. It is rational to share the cost and risks of this new innovation through creation, storage, transfer and application of knowledge among the partners of the innovation ecosystem. There are different modes of collaboration such as strategic alliance, joint ventures, technology licensing, outsourcing and collective research organizations. Collaborative networks are other sources of innovation. Collaboration is facilitated by geographical proximity, regional technology clusters and technology spillovers. Technological spillover results from the spread of knowledge across organizational or regional boundaries; it occurs when the benefits from R&D activities of a firm spill over to other firms. But, it may be hard to control the development of product and process innovation protecting IP of

proprietary technologies. The critical success factors of collaborative networks may be right selection of innovation partners having strategic and resource fit, transparent and flexible monitoring and governance process so that the innovation partners understand their rights and obligations.

The technological innovation of EVs demands the motivation and commitment of creative people. It is not a trivial problem; need useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. The impact of knowledge on creativity is double-edged. Lack of knowledge is a major constraint to the original contribution in a technological innovation. A creative person is expected to have confidence in own capabilities, tolerance for ambiguity, interest in solving problems and willingness to overcome obstacles by taking reasonable risks. A cooperative and collaborative environment must recognize and reward creative talent in time.

The sources of RailTech innovation may be R&D units of Railways Corporation, MIS and IT units of engineering and management institutes and collaborative networks. Creativity is the underlying process for RailTech innovation which can promote new ideas through shared vision, intellectual abilities, thinking style, knowledge, personality, motivation, commitment, confidence and group dynamics. It demands the motivation and commitment of the creative people to look at the problems in unconventional ways. Organizational creativity is closely associated with human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy, organization structure, corporate culture, routine and incentive policy.

7.SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- **New *skills* developments for EV drivers, battery charging stations and traffic controller**
  - **Data visualization and data analysis Information and communication technology,**
  - **Battery charging**
  - **Coordination and integration in traffic control;**
  - **knowledge of operation and best practices of vehicle manufacturing, robotics, technical, system administration, management, governance, supply chain management;**
  - **New skills developments for train drivers and traffic controller**
  - **Data visualization and data analysis (e.g. fault tree, FMEA, TFPG)**
  - **Information and communication technology,**
  - **Coordination and integration in traffic control;**
- ***Style*** **: Project management by objectives, shared vision and goal setting; leadership, shared vision, goal setting, intelligent communication, risk assessment and mitigation, innovation project management; energy efficient**

driving style, operation management by objectives, shared vision and goal setting

- ***Support*** **: proactive, reactive, preventive and breakdown maintenance of EVs system (e.g. mechanical, electrical, electronics and IT schema); proactive, reactive, preventive and breakdown maintenance of RailTech system (e.g. mechanical, electrical, electronics and IT schema;**
- **Audit gaps in skills, style and support through rational talent acquisition, retention and training strategies.**

Finally, Dr. Prakash is discussing on ‘skill-style-support’ for logistics security. The workforce involved in EVs innovation are expected to develop different types of skills in technical (e.g. battery charging, solar power, hybrid vehicles), management and system administration domains such as research and development, maintenance support, knowledge management, system design, process innovation and project management. The system administrators should have leadership skill in smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of EVs innovation demands the support of effective leadership style. It is really challenging for the project leaders to implement top technology innovations physically and practically. Top management should be able to tackle the complexity of system implementation with the support of efficient teams.

It is essential to develop multiple skills in new EVs system development through proper coordination among design and supply chains. The basic objectives are to maximize fit with the needs of the drivers, ensure quality assurance and control R&D cost. It is an interesting option to get the suppliers and the drivers in the development process. It is really challenging to develop a complex EV system through a sound knowledge base and problem solving capability.

What should be the right organization model for this technological innovation? A traditional functionally centered organization model may not be suitable for supporting end-to-end business processes. Such process management is more than a way to improve the performance of individual processes; it is a way to operate and manage a business. An enterprise that has institutionalized process management and aligned management systems to support is a process enterprise. It is centered on its customers, managed around its processes and is aligned around a common, customer oriented goal. The business models of EVs require the support of a process enterprise structure enabled with advanced information and communication technology. The structure should have project, design, production, supply chain management maintenance, human resource management, sales & marketing and finance cells. The structure should be governed by an executive committee comprising of CEO and directors. The process managers should be able to identify core processes in the value chain; communicate throughout the organization about these critical processes; create and deploy measures regarding end-to-end process performance and define process owners with end-to-end authority for process design, resource procurement, process monitoring for redesign and improvement.

The structure of process enterprise requires a collaborative and cooperative work culture. Top innovations need proactive, reactive and preventive support for proper technology management.

What should be the innovation model for effective diffusion of Railtech security? Is it possible to adopt K-A-B-C-D-E-T-F model? The workforce involved in RailTech innovation are expected to develop different types of skills in technical (e.g. MIS, information and communication technology), management and system administration domains such as research and development, maintenance support, knowledge management, system design, process innovation and project management. The system administrators should have leadership skill in smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of RailTech innovation demands the support of effective leadership style. It is really challenging for the project leaders to implement top technology innovations physically and practically. Top management should be able to tackle the complexity of system implementation with the support of efficient teams.

It is essential to develop multiple skills in new RailTech system development through proper coordination among design and supply chains. The basic objectives are to maximize fit with the needs of the drivers, ensure quality assurance and control R&D cost. It is an interesting option to get the suppliers and the train drivers in the development process. It is really challenging to develop a complex RailTech system through a sound knowledge base and problem solving capability.

8. CONCLUSION

What must be done to realize the future vision of EVs? It is essential to manage the fit among the design of EVs, energy and communication infrastructure and corporate governance; form coalition of the stakeholders; explore intelligent mechanisms and build a broad consensus around a common vision. There are critical issues such as purchasing dynamics and shared mobility. The preference of young generation has been changing. It is also essential to define a rational Govt. policy for the innovation, adoption and diffusion of EVs such as development of battery charging infrastructure, rationalization of profit margin of the manufacturers and dealers of EVs and reduction of tax. It is also necessary to stimulate the political support and consumer demand through SWOT analysis, what is at stake and what is possible, threats analysis and risk mitigation strategies. It may be interesting to launch a set of pilot projects at sufficient scale and investment to enable the integration of the key innovative solutions of electrical and hybrid vehicles. The aforesaid problem is an extremely complex issue in the world since we are not rich and blessed with adequate supply of natural resources in oil and gas sector; the situation demands proper coordination and integration among seven 'S' factors of deep analytics.

How to manage evolution of technological innovation in RailTech security and safety, specifically for long distance trains? The nature of innovation is expected to

shift after the emergence of a dominant design. The pace of improvement of RailTech performance should be monitored properly. The evolution of this innovation is influenced by intersecting trajectories of performance as demanded by the drivers and the performance supplied by RailTech system. The diffusion of innovation depends on how the new technology will spread through a population of potential adopters globally. The present work considers only a specific area of RailTech with focus on DAS and real-time fault diagnostics from the perspectives of MIS. It is really an interesting and potential research agenda. It is possible to extend this study in various ways. Is it rational to imagine a train as a block chain? There are other various issues of RailTech safety and security such as consistency in train length, fire hazards, food poisoning, health & hygiene issues, anti-collision devices, modernization of rail signaling system, smart coaches, smart grid, black box, use of CCTV/Wi-Fi/Webcam, unmanned level crossing, passengers crossing railway tracks while talking on mobile phones, derailment of trains due to cracks in tracks or poor maintenance, rushing attacks, non-availability of overbridges, footbridges and skywalks and miscellaneous flaws in mechanical, electrical and civil infrastructure. Is it possible to extend this study to the decision making problems of external and home affairs ministries in corporate governance such as human traffic and refugees control in a country? An intelligent rail budget is expected to address all these issues rationally.

FURTHER READING

- **U.Eberle and R.V. Helmolt. 2010. Sustainable transportation based on electrical vehicle concepts : a brief review. Energy & Environmental Science, 3, 680-699.**
- **K. Girotra and S. Netessine. 2011. The electrical vehicle renaissance: Better place Inc. Teaching case. INSEAD.**
- **BCG report 2010. Batteries for electric cars. Challenges, opportunities and the outlook to 2020.**
- **V. Robu, E.H. Gerding, S. Stein, D.C. Parkes, A. Rogers & N.R.Jennings. 2013. An online mechanism for multi-unit demand and its application to plug-in hybrid electric vehicle charging. Journal of Artificial Intelligence Research, 48, 175-230.**
- **H.Stromberg, P.Andersson, S. Almgren, J. Ericsson, M. Karlsson & A. Nabo. 2011. Driver interfaces for electric vehicles. In Proceedings of the 3rd International Conference on Automotive User Interfaces and Interactive Vehicular Applications, AutomotiveUI '11, pp. 177-184, New York, NY, USA. ACM.**
- **C. Ahn, C.Li and H.Peng. 2011. Optimal decentralized charging control algorithm for electrified vehicles connected to smart grid. Journal of Power Sources, 196 (23), 10369 - 10379.**
- **K. Clement-Nyns, E. Haesen and J. Driesen. 2010. The impact of charging plug-in hybrid electric vehicles on a residential distribution grid. IEEE Transactions on Power Systems, 25 (1), 371- 380.**

- C.M. Flath, J.P. Ilg, S. Gottwalt, H. Schmeck and C. Weinhardt. 2014. Improving electric vehicle charging coordination through area pricing. Transportation Science, 48 (4), 619-634.
- K. Hayakawa, E. Gerding, S. Stein and T. Shiga. 2015. Online mechanisms for charging electric vehicles in settings with varying marginal electricity costs. In 24th International Joint Conference on Artificial Intelligence (IJCAI), pp. 2610-2616.
- M. Granovskii, I. Dincer, M.A. Rosen, J. Power Sources 159. 2006. 1186.
- C. Zamfirescu, I. Dincer, J. Power Sources 185. 2008. 459.
- C. Zamfirescu, I. Dincer, Fuel Process. Technology. 90. 2009. 729.
- C. Handley, N. Brandon, R. Vorst, J. Power Sources 106. 2002. 344.
- P. Van den Bossche. 2003. The Electric Vehicle: Raising the Standards. Ph.D. Thesis, Vrije Universiteit Brussel.
- D.L.Burns, B. McCormick and C.E. Borroni-Bird. Vehicle of Change. 2002. Scientific American 287 : 64 – 73.
- L. Burns. 1993. Busy Bodies: Why Our Time-Obsessed Society Keeps Us Running in Place . New York : Norton.
- W.J. Mitchell. 1994. City of Bits: Space, Place, and the Infobahn .Cambridge, M ass. : MIT Press.
- W.J.Mitchell. 1999. E-topia . Cambridge, Mass. : MIT Press.
- W.J.Mitchell. 2004. Me++: The Cyborg Self and the Networked City . Cambridge, M ass. : MIT Press.
- R.L.Ackoff, J. Magidson and J.A. Herbert. 2006. Idealized Design: How to Dissolve Tomorrow's Crisis Today. Upper Saddle River, N .J. : Wharton School Publishing.
- R. Adams and T. Brewer. 2004. A Plan for 21st Century Land Transport. International Journal of Vehicle Design 35 (1/2) : 137 – 150.
- J.H.Ausubel, C. Marchetti and P. Meyer. 1998. Toward Green Mobility: Th e Evolution of Transport. " European Review 6 (2) (1998): 137 – 156.
- G.Boyle, ed. 2004. Renewable Energy . Oxford University Press.
- G. Boyle, ed. 2007. Renewable Energy and the Grid: The Challenge of Variability . London : Earthscan Publications.
- G.Boyle, B. Everett, and J. Ramage. 2003. Energy Systems and Sustainability . Oxford University Press.
- R. Brandon. 2002 Auto Mobile: How the Car Changed Life. London : Macmillan .
- C.M.Christenson. 1997. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail . Cambridge, Mass. : Harvard B usiness School Press.
- P. Droege. 2006. The Renewable City: A Comprehensive Guide to an Urban Revolution . Chichester : Wiley.
- P.Droege. 2008. Urban Energy Transition: From Fossil Fuels to Renewable Power . Oxford : Elsevier Science.
- S. Grava. 2003. Urban Transportation Systems . New York : McGraw-Hill.

- **S.Henley. 2007. The Architecture of Parking . New York : Thames and Hudson.**
- **I.M. Hoffert , K. Caldeira , G. Benford , D. R. Criswell, C. Green , H. Herzog, A. K. Jain, H. S. Kheshgi, K. S. Lackner, J.S. Lewis , H. D. Lightfoot, W. Manheimer, J. C. Mankins , M. E. Mauel , L. J. Perkins , M. E. Schlesinger , T. Volk and T. M. L. Wigley. 2002. Advanced Technology Paths to Global Climate Stability: Energy for a Greenhouse Planet. Science 298 (5595) : 981 – 987.**
- **D.A. Kirsch. 2000. The Electric Vehicle and the Burden of History. New B runswick, N .J. : Rutgers University Press.**
- **Ladd , Brian. 2008. Autophobia: Love and Hate in the Automobile Age . Chicago : University o f Chicago Press.**
- **D. Mohan . 2008. Mythologies, Metros, and Future Urban Transport . TRIPP Report 08-01. New Delhi: Transportation Research and Injury Prevention Program.**
- **G. Mom. 2004. The Electric Vehicle: Technology and Expectations in the Automobile Age . Baltimore : Johns Hopkins University Press.**
- **R.A.Popa, H. Balakrishnan and A. J. Blumberg. 2009. VPriv: Protecting Privacy in Location-Based Vehicle Services. 18th USENIX Security Symposium. Montreal,August.**
- **M. Safdie and W. Kohn. 1998. The City After the Automobile: An Architect's Vision . Boulder, C olo. : Westview Press.**
- **R. Strzelecki and B. Grzegorz eds. 2008. Power Electronics in Smart Electrical Energy Networks . London : Springer.**
- **J. Weinert, M.Chaktan and C. Cherry. 2007. The Transition to Electric Bikes in China and Key Reasons for Rapid Growth " Transportation 34: 301 – 318 .**
- **M.A. Weiss, J. B. Heywood, E.M.Drake , A. Schafer and F.F. AuYeung. 2000. On the Road in 2020: A Life-Cycle Analysis of New Automobile Technologies. Energy Laboratory Report MIT EL 00-003. Energy Laboratory, MIT. October.**
- **D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010.**
- **T. Albrecht. 2005. Energy-efficient train control in suburban railways: experiences gained from onboard tests of a driver assistance system. In: 1st International Seminar on Railway Operations Modelling and Analysis, Delft, Netherlands.**
- **T. Albrecht. 2009. The influence of anticipating train driving on the dispatching process in railway conflict situations. Netw. Spat. Econ. 9 (1), 85.**
- **T. Albrecht. 2013. Human factor challenges in the development of a driver advisory system for regional passenger trains. In: Rail Human Factors: Supporting Reliability, Safety and Cost Reduction, pp. 129–138.**
- **S.Dekker. 2007. Conflict detection and human-machine coordination. In: Hindsight, 4, January 2007. EUROCONTROL Directorate of ATM**

Programme – Security, Safety and Human Factors Business Division (DAP/SSH), pp 7–9.

- **DeltaRail Group. 2008. Advisory speeds for drivers for energy management and regulation. In: RSSB Interim Report Milestone 2, Issue 01 and 02.**
- **DeltaRail Group. 2009. Driver advisory information for energy management and regulation. In: Stage 1 Report, RSSB Research Programme, T724.**
- **W. Hamilton and T. Clarke. 2005. Driver performance modelling and its practical application to railway safety. Appl. Ergon. 36 (6), 661–670.**
- **P.G.Howlett, I.P. Milroy and P.J. Pudney. 1994. Energy-efficient train control. Control Eng. Pract. 2 (2), 193–200.**
- **R. Liu AND I.M. Golovitcher. 2003. Energy-efficient operation of rail vehicles. Transp.Res. A 37, 917–932.**
- **P. Lukaszewicz. 2008. Methods for energy efficient driving – algorithms. RailEnergy, Document ID NRG-KTH-D-2.3-005.**
- **I. Mitchell. 2009. The sustainable railway: use of advisory systems for energy savings. IRSE News, No.151, pp. 2–7.**
- **Rail Safety and Standards Board, 2008. The Rule Book. GE/RT8000, Issue 7.**
- **Rail Safety & Standards Board,2008. Good Practice Guide To Train Driver Training.RS/221,Issue 1.**
- **Rail Safety and Standards Board, 2008. Train Movement – Staff Suitability and Fitness Requirements, GO/RT3451, Issue 01.**
- **S. Tschirner, S., A.W.Andersson and B. Sandblad. 2013. Designing train driver advisory systems for situation awareness. In: Rail Human Factors: Supporting Reliability,Safety and Cost Reduction. pp.150–159.**
- **J. Wardale. 2008. Advice on energy efficient driving. Presentation to drivers, CrossCountry Rail.**
- **C.Conte and A. Schöbel. 2007. Identifying dependencies among delays. In: Proceedings of 2nd International Seminar on Railway Operations Research (RailHannover 2007), Hannover.**
- **W.Daamen, T. Houben, R.M.P. Goverde, I.A. Hansen, V.A. Weeda. 2006. Monitoring system for reliability of rail transport chains. In: Proceedings of the 7th World Congress on Railway Research (WCRR 2006), Montreal.**
- **S. De Fabris, G.Longo and G. Medeossi. 2008. Automated analysis of train event recorder data to improve micro-simulation models. In: J. Allan, E. Arias, C.A. Brebbia, C. Goodman, A.F. Rumsey, G. Sciutto, G. and A. Tomii (Eds.), Computers in Railways XI. WIT Press, Southampton, 575–583.**
- **A. Exer. 1995. Rail traffic management. In: Bailey, C. (Ed.), European Railway Signalling. IRSE, A&C Black, London, 311–342.**
- **H. Flier, R. Gelashvili, R., T. Graffagnino and M. Nunkesser. 2009. Mining railway delay dependencies in large-scale real-world delay data. In: Ahuja, R.K., Möhring, R.H., Zaroliagis, C.D. (Eds.), Robust and Online Large-Scale Optimization: Models and Techniques for Transportation Systems, LNCS 5868. Springer, Berlin, 354–368.**
- **R.M.P. Goverde. 2005. Punctuality of railway operations and timetable stability analysis. PhD thesis, Delft University of Technology.**

- **R.M.P.Goverde. 2011. A delay propagation algorithm for large-scale railway traffic networks. Transportation Research, Part C 18 (3), 269–287.**
- **R.M.P.Goverde, W. Daamen, I.A. Hansen, I.A. 2008. Automatic identification of route conflict occurrences and their consequences. In: Allan, J., Arias, E., Brebbia, C.A.,Goodman, C., Rumsey, A.F., Sciutto, G., Tomii, A. (Eds.), Computers in Railways XI. WIT Press, Southampton, pp. 473–482.**
- **P.Konstantinos, P. Tzieropoulos and D. Emery. 2014. Railway driver advice systems: Evaluation of methods, tools and systems. Journal of Rail Transport Planning & Management.**
- **M.Ullius. 2004. Verwendung von Eisenbahnbetriebsdaten für die Schwachstellenund Risikoanalyse zur Verbesserung der Angebots- und Betriebsqualität. PhD thesis, Swiss Federal Institute of Technology, Zurich.**
- **N.Van Oort. 2011. Service reliability and urban public transport design. PhD thesis, Delft University of Technology.**
- **Fault Tree Analysis, CEI/IEC 61025:2006.**
- **S. Padalkar, J. Sztipanovits, G. Karsai, N. Miyasaka and K. C. Okuda. 1991. Real-time fault diagnostics. IEEE Expert, vol. 6, no. 3, pp. 75–85.**
- **A.Misra, J.Sztipanovits, A. Underbrink, R. Carnes and B. Purves. 1992. Diagnosability of dynamical systems. In 3rd International Workshop on Principles of Diagnosis.**
- **A.Misra. 1994. Senor-based diagnosis of dynamical systems. Ph.D. Dissertation, Vanderbilt University.**
- **S.C.Ofsthun and S. Abdelwahed. 2007. Practical applications of timed failure propagation graphs for vehicle diagnosis. In Autotestcon, 2007 IEEE, 250–259.**
- **S. Abdelwahed, G. Karsai and G. Biswas.2006. Notions of Diagnosability for Timed Failure Propagation Graphs. In IEEE Systems Readiness Technology Conference, AUTOTESTCON'06, CA.**
- **R.Alur, and T.A. Henzinger. 1993. Real-time logics: complexity and expressiveness. Information and Computation 104(1):35–77.**
- **B.Bittner, M.Bozzano, A. Cimatti, M.Gario and A.Griggio. 2014. Towards pareto-optimal parameter synthesis for monotonic cost functions. In Proceedings of the 14th Conference on Formal Methods in Computer-Aided Design, 23–30.**
- **B. Bittner, M. Bozzano, R.Cavada, A. Cimatti, M.Gario, A. Griggio, C. Mattarei, A. Micheli, and G. Zampedri. 2015. The xSAP safety analysis platform. arXiv preprint arXiv:1504.07513.**
- **M. Bozzano, A. Cimatti, A. Pires, D. Jones, G. Kimberly, T. Petri, R. Robinson, and S. Tonetta. 2015. Formal Design and Safety Analysis of AIR6110 Wheel Brake System. In Proc. CAV 2015, 518–535.**
- **M. Bozzano, A. Cimatti, M. Gario and A.Micheli. 2015. Smt-based validation of timed failure propagation graphs. In 29th AAAI Conference on Artificial Intelligence.**

- **M.Bozzano, A. Cimatti and f. Tapparo. 2007. Symbolic fault tree analysis for reactive systems. In Automated Technology for Verification and Analysis, Springer, 162–176.**
- **R. Cavada, A. Cimatti, M. Dorigatti, A. Griggio, A. Mariotti, A. Micheli, S. Mover, M. Roveri and S. Tonetta. 2014. The nuxmv symbolic model checker. In Computer Aided Verification.334–342. Springer.**
- **C. Roberts and R.M.Goodall. 2009. Strategies and techniques for safety and performance monitoring on railways. Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Spain.**

Quiz

- **Justify EVs & HVs as a technology for humanity. What is the scope of this technology?**
- **What is the dominant design of the technology related to EVs / HVs?**
- **What are the basic elements of the system architecture of EVs / HVs?**
- **What do you mean by technology security of EVs / HVs? How can You verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion for EVs & HVs'? What is the outcome of technology life-cycle analysis and SWOT analysis of conventional and electrical vehicles?**
- **How to manage resources for innovation project of EVs / HVs?**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How do You manage technology innovation project efficiently for EVs/ HVs? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
- **Design smart battery for EVs / HVs.**
- **Evaluate the scope of V2V communication and IoT technology for the security of future generation vehicles.**
- **Explain the technology of Railtech Security and Safety? Justify it as a technology for humanity. What is the scope of this technology?**
- **What is the dominant design of rail DAS?**
- **What are the basic elements of the system architecture rail DAS?**
- **How should you manage resources for railtech innovation project?**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by railtech innovation?**
- **How should You manage railtech innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
- **Design an optimal DAS architecture through SWOT analysis.**
- **Design Real-time Fault Diagnostics which can be integrated with DAS.**
- **What are the strategic moves of technology innovation, adoption and diffusion for Railtech Security and Safety'? What is the outcome of**

technology life-cycle analysis? What do you mean by railtech security? How do You verify the security intelligence? Please refer to following cases.

- **Please study following 5 cases and suggest suitable technological solutions.**

Test case 1 (Fire in metro rail) **: It was an incident of fire in metro rail of the metropolitan city Sidben.**

19:02 : Trip of electrical connection near Masco station, suffocating black smoke was spreading rapidly inside the tunnel of metro rail.

19:03: The information was given to the fire brigade and police. The helpless passengers were trapped inside the locked and fully packed metro rail compartments; they were traumatized; it was a horrific experience; the time lasted for 55 minutes; the passengers tried to escape from the locked compartments by breaking glass windows but could not be successful; some passengers were injured in stampede; they called metro rail helpline, the public address system did not work; a passenger broke her leg; the metro rail boards and the state governments were involved in blame game; the metro rail board set up a committee. The metro rail wrecks are in dangerous conditions; there was no proper maintenance; anything from the rail compartment falling on the rail track might cause fire.

19:05: The metro rail employees started extinguishing fire by spraying water.

19: 14 : The electrical supply was disconnected in third rail.

19: 20 : The emergency rescue operation started.

19:55 : The rescue operation ended.

Deep analytics raised a set of important issues on the aforesaid accident in metro rail:

- **Was the disaster management team ready to control the situation? What was the composition of disaster management team: NDRF, NSG and the employees of metro rail?**
- **What was the response time in such type of disaster? What are the devices and equipments available: jacket, gas mask, oxygen cylinders or anything else?**
- **What were the fire protection strategies? Can the employees of rail stations tackle small fire incidents? Can the fire brigade tackle major fire accidents? Are there water pipes in the tunnel for extinguishing fire?**
- **Is it possible to save the passengers from various acts of terrorism through the efforts of the police, military and NSG?**
- **Did the public address system work correctly in time?**
- **Was the logic of emergency door opening correct: was it a fully automated or manual system? Did the doors open only at station platforms?**
- **Was the maintenance problem considered as the root cause of the accident?**
- **Was there high risk of accidents in the metro rail? Who should be punished for the irresponsibilities? What was the accountability of higher authorities? Who took the responsibilities of any damage of the passengers?**
- **Why did not the driver drive the train towards next station from the spot of accident? Why did the train stop in the tunnel?**
- **Why did the emergency brake work? Was it due to the disconnection of power supply in train protection circuit?**

- **Was the driver able to contact the control room?**
- **Did the passengers get down before the disconnection of power supply in the third rail?**
- **Where were the train driver and guard during the time of accident?**
- **Was there any metro rail helpline number; how to contact the control room?**

The possible risk mitigation strategies are expected to include several critical measures such as fire protection system, smoke detectors and CCTVs in each compartment, regulatory compliance on smoking inside running train, ban on carrying of hazardous materials (e.g. bombs, fireworks, explosives, kerosene, petrol and diesel) by the passengers, fire protection from the gas oven at pantry cars, use of induction cookers instead of gas ovens, announcements and alerts in time through public address system, automated air conditioning system in the tunnel, automated control of the velocity and direction of airflow to resist spreading of smoke and fire, automated airflow control system in the compartment after sensing smoke, footpath inside the tunnel, disconnection of power supply in third rail, fire caused by antisocialists and terrorists such as explosion or nerve gas attack and readiness of fire brigade and disaster management workforce. There are other problems of sensors enabled automatic closing of the doors of metro trains. A door may remain open during running condition. On the contrary, a door may be closed during stoppage at a station. Such types of problems occur due to the malfunctioning of limit switches.

Test case 2 (Fog and mist in winter) **: It was winter in January'2018. Smith was pursuing his Doctoral programme at a management institute. He went to Nelhi to present his paper at an International Conference. He was accompanied with his mother (50 years), wife (35 years) and son (3 years). It was a very cold night. Smith was returning to Cowrah from Nelhi by a superfast mail. The train started at 1 a.m. with a delay of 4 hours. The train arrived near Panpur and stopped. The reason was poor visibility to the train driver due to dense fog and mist. The temperature was about 2 degree centigrade. The train could not start for about 4 hours till the sunrise in the morning. It was a horrible experience to Smith and his family members. They were in non-AC compartment. The kids inside the train compartment were crying and coughing in the severe cold weather. All the passengers and the driver were helpless at that night.**

Test case 3 (Breakdown during journey)**: Smith was returning from Hennai to Cowrah by a superfast express train. The train started at 23-45. At midnight, the train suddenly halted with heavy jerk. The passengers became frightened. The driver discovered that the gas pipe was broken. He replaced the gas pipe through shearing and welding operations in the darkness. The train was delayed by 1 hour. Was it possible to predict the poor health of the gas pipe in time?**

Test case 4 (Act of terrorism)**: There were rail accidents with many casualties in country X due to various acts of terrorism. One case, the fishplates were taken out by the terrorists. There were five cases where the railway tracks were blown out with highly dangerous explosive bombs by the malicious agents. There were some**

horrific incidents of robbery and loot by the dacoits at night. There were also many incidents of theft of shoes and belongings of the passengers. Can automated check-in system at various rail stations ensure security and safety of the passengers? Do the passengers need protection by the armed security force and watchdogs during journey by rail?

***Test case 5 (Healthcare problem during rail journey)*: There were frequent cases of allergic disorders, itching, skin rash, heart burning, stomach upset, loose motion and food poisoning of the train passengers during long distance rail journey in summer and also cold and cough, breathing problems and fever in winter. There are high risks of attacks of infectious diseases (e.g. conjunctivitis, eye infection, skin rashes etc) from other travelers during rail travel. Should the passengers carry emergency medicines (e.g. anti-allergic tablets, fever, cold and cough, digestion problem, stomach upset) and pure drinking water as proactive and reactive approaches of healthcare? Should they avoid spicy, oily, rich and fast food during travel? Railway catering services must take care of such issues. The travelers should clean their seats and berths with disinfection germ protection cleaning agents proactively. During epidemic and pandemic disaster, railways authorities should arrange quarantined compartments of each long distance train for contact isolation of the travelers and passengers. They should also broadcast the aforesaid precautionary measures to the travelers and passengers through intelligent broadcast communication channels.**

SESSION 8: TECHNOLOGIES for HUMANITY - FINANCIAL SECURITY & PROOF OF WORKS

Abstract:
Event **: Technology for humanity and global security summit**
Venue**: Financial security hall, Technology park : Sanada**
Time Schedule **: 2 p.m. – 5 p.m. , 17.8.2020**
Agents **: Representatives of various global organizations (Global nations, global financial organization, global economic forum), Technology management experts from science and technology forums, financial engineers, scientists, representatives and ministers from the departments of finance of developed, developing and underdeveloped countries, CEOs of financial corporations, business development consultants, reprentatives from NGOs.**
Topic of discussion and key focus areas**: financial security, fault attacks, proof of works, block chain, mobile commerce.**
Keynote speakers**: Prof. S. Ramaswamy, Prof. Daniel Parker, Prof. G. Nissim, Prof. Harry Goldwasser, Prof. M. Sandholm, Dr. Richarson, Dr. Nakamoto, Dr. Shi, Dr. Sarapova**

1. SCOPE

Scope Analytics
Agents**: Scientists, system analysts, financial analysts;**
Moves **: Critical success factors analysis, Requirements management;**
Security parameters**: Define a set of sustainable development goals for financial security.**

- **Banking**
- **Financial services (postal, mutual fund, bond)**
- **Tax**
- **Insurance (general, life, health)**
- **Retirement planning**
- **Stock and derivatives trading**

Dr. Parker is analyzing financial security from the perspectives of technology, business and government. The emerging technology is analyzed through '7-S' model : Scope, System, Structure, Security, Strategy, Staff-resources and Skill-Style-Support.. The technology is applicable to various interesting areas such as anti-money laundering, insurance, stock trading, portfolio management, crypto currencies, banking and financial services. The system for the technology has been analyzed in terms of business analytics, big data analytics, data visualization and performance scorecard. Structure is focused on computing, data, networking and application schema of financial system. Security explores various aspects of fairness, correctness, authentication, authorization, correct identification, privacy and audit of financial data. The strategy of innovation, adoption and diffusion debates whether the technology is an evolution or

revolution through SWOT analysis and technology life-cycle analysis. The technology is at emergence phase of S-Curve. It has been evolving with advancement of digital technologies such as web, cloud computing, internet, mobile communication, tablets, laptops and desktop computers and intelligent software (e.g. analytics, data visualization). On the other side, the technology is facing several challenges today in terms of regulatory compliance and creation of new job opportunities. The technology demands the availability of skilled resources such as business analysts, big data analysts, digital system administrators and support staff.

2. SYSTEM

System Analytics

***Agents*: system analysts, business analysts, scientists;**

***Moves* : requirements engineering, system design, coding, prototype testing, installation, testing, commissioning**

***Emerging technologies*: Innovate a set of emerging digital technologies to ensure financial security such as anti-money laundering, fraud detection, proof of works, secure multi-party computation and financial analytics;**

Prof. G. Nissim and Prof. Goldwasser are outlining the system associated with the technology of financial security. Financial analytics is an intelligent, complex, hybrid, multi-phased and multi-dimensional data analysis system. The basic steps of computation are data sourcing, data filtering / preprocessing, data ensembling, data analysis and knowledge discovery from data. The authorized data analysts select an optimal set of input variables, features and dimensions (e.g. scope, system, structure, security, strategy, staff-resources, skill-style-support) correctly being free from malicious attacks (e.g. false data injection, shilling); input data is sourced through authenticated channels accordingly. The sourced data is filtered, preprocessed (e.g. bagging, boosting, cross validation) and ensembled. It is rational to adopt an optimal mix of quantitative (e.g. regression, prediction, sequence, association, classification and clustering algorithms) and qualitative methods for multi-dimensional analysis. The analysts define intelligent training and testing strategies in terms of selection of correct soft computing tools, network architecture – no. of layers and nodes; training algorithm, learning rate, no. of training rounds, cross validation and stopping criteria. The hidden knowledge is discovered from data in terms of business intelligence. The analysts audit fairness and correctness of computation and also reliability, consistency, rationality, transparency and accountability of the analytics.

Financial analytics can process precisely targeted, complex and fast queries on large data sets of real-time and near real-time systems. Business analytics follows a systematic, streamlined and structured process that can extract, organize and analyze large amounts of data in a form being acceptable, useful and beneficial for an entity. It is basically a specific type of distributed computing across a number of server or nodes to speed up the analysis process. Generally, shallow analytics use the concept of means, standard deviation, variance, probability, proportions, pie charts,

bar charts and tabs to analyze small data set. Business analytics analyze large data sets based on the concepts of data visualization, descriptive and prescriptive statistics, predictive modeling, machine learning, multilevel modeling, data reduction, multivariate analysis, regression analysis, logistic regression analysis, text analysis and data wrangling. Deep analytics is often coupled with business intelligence applications which perform query based search on large data, analyze, extract information from data sets hosted on a complex and distributed architecture and convert that information into specialized data visualization outcome such as reports, charts and graphs. Big data refers to large data being generated continuously in the form of unstructured, semi-structured and structured data produced by social network to scientific computing applications. The dataset may range from a few hundred gigabytes to terabytes beyond the capacity of existing data management tools that can capture, store, manage and analyze. Big data is characterized by volume, velocity, variety, variability, complexity and low value density. Capital market firms use big data technologies to mitigate risks for fraud mitigation, ondemand enterprise management, regulation, trading analysis and data tagging.

3. STRUCTURE

Structure Analytics

***Agents*: system analysts, business analysts;**

***Moves*: Design and configure**

- **Organization structure**
    - **Technology forums**
    - **National level : Government (E-governance model), NGOs, research organizations;**
    - **International level : strategic alliance among global organizations (nations, heath, child, peace);**
- **System architecture (topology, modules, nodes, connectivity, layers);**
    - ***Emerging technologies* : Innovate a set of emerging technologies as per the goals of financial security;**
    - ***Level 1*: digital technology, information technology, computer science, electrical, electronics, telecommunication, civil ;**
    - ***Level 2*: Identify fundamental building blocks of information technology:**
        - **computing**
        - **data (data warehouses, big data analytics, performance scorecard)**
        - **networking (web connectivity)**
        - **security schema**
        - **application schema**

Prof. Sandholm is analyzing the structure i.e. the backbone of a system associated with a specific technological innovation on financial security. What are the basic elements of the system architecture associated with FINTECH? It has five critical

viewpoints: computing, data, networking, application and security schema. The topology of the system architecture may be analyzed in terms of nodes, connectivity, type of connections, layers, interfaces between layers and organization of layers.

4. SECURITY

Security Analytics

***Verification mechanism*: audit *security intelligence* through intelligent *surveillance technologies*.**

- ***multi-party corruption:* do surveillance through security council of global organization, police, army, detectives, journalists ;**
- ***access control*: verify authentication, authorization, correct identification, privacy, audit confidentiality, data integrity and non-repudiation;**
- **financial security policy: verify rationality, fairness, correctness, transparency, accountability, trust and commitment;**
- ***system performance:* verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness, reachability, synchronization, safety;**
- ***malicious attacks*: verify the risk of Sybil, false data injection, shilling: push and pull, denial of service (DoS), fault injection attack;**
- ***web security:* session hijack, phishing, hacking, cross site request forgery, cross site script, broken authentication, improper error handling;**

call threat analytics and assess risks of emerging financial technologies :

- **what is corrupted or compromised (agents, computing schema, communication schema, data schema, application schema)? detect type of threat.**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights : how and why did it occur? do cause-effect analysis on performance, sensitivity, trends, exception and alerts.**
- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**

***Output*: security intelligence**

Prof. Ramaswamy and Dr. Nakamoto are analyzing the security of emerging banking, postal and financial services. The security intelligence of financial system is a multi-dimensional parameter which should be verified at various levels. The regulatory clauses should be defined and audited by a group of authorized agents correctly and rationally. It is crucial to verify and evaluate various rules and regulatory clauses for financial security in terms of fairness, correctness, rationality, transparency, accountability, commitment and trust. It is essential to evaluate the performance of the system in terms of reliability, consistency, and stability. The performance of the system is expected to be consistent and reliable. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that the system should never be in a state in which no progress is possible. The system should be protected from various types of internal and external

malicious attacks such as false data injection, Sybil, shilling and denial of service (DoS) attack. The auditors must assess the threats of such types of malicious attacks by adversaries. It is also important to assess the risk of multi-party corruptions on the financial security technologies in terms of agents, policy, procedure and protocol. An efficient knowledge based system is expected to monitor the gaps and violations in regulatory compliance in real-time and diagnose any fault just like supervisory control and data acquisition system. Dr. Ramaswamy is analyzing the following case during today's age of technology transition.

Case : Fault attacks and proof of works in banking, postal and financial services

"

Feedback - Technical problems and operational issues at your post offices and banks at Talkia, Cowrah 811106

To: Mrs. Darithi Thatcher, Minister of Finance, Govt. of Vindia,

CC: Mr. Tony Lucas, The Manager, State bank of Vindia, Talkia; Mr. Rineet Sandey, Director General, Post, Govt. of Vindia, Ms. Smita Kugar, Member, Technology; Dr. Charles Lamb, Member Operation, Mr. Madpita Rosui, Chairperson, Postal Service Board

The Postmaster, Post Office – Talkia, Cowrah – 811106;

Respected Sir / Madam,

We, the residents of Talkia have been experiencing various type of quality of service and operational problems such as delay in service and long queues due to technical errors and malfunctioning of Internet connectivity, printer, monitor and other hardware devices at local banks and post offices in Talkia, Vindia. There is shortage of postcards and envelops at post offices. We are getting misleading SMS message from your post offices with incorrect account balances, sometimes we are not getting important SMS messages related to high valued transactions; there are cases of messages drop, denial of service and fault attacks. This is basically the problem of your information and communication system.

We would also like to elaborate and clarify the problems related to your operations, information and communication system in terms of workplace safety, fairness, correctness, transparency, Sybil attack and accountability through following illustrations.

a) Leakage of water from the roof of your post office damaging important documents and systems, particularly during rain

b) During printing of savings passbook, the last digit of new MIS (Monthly Income Savings) account number is not getting printed due to the problem of your information system. The printing is not transparent and is very hedgy; there is also alignment problem. It is basically the fault related to your proof of works.

c) The color of new MIS passbook's front and back cover is not matching with your logo (red and yellow); it is now (red + light pink); the name of 'printed by' of the passbook at last page is also missing.

d) Nominee field is blank in the passbooks though the information was given during opening of accounts by the applicants.

Request your intervention for necessary corrective actions on immediate basis forour relief.

Regards.
L.R. Bukla, MLA, Talkia
"

Financial systems may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging financial technology demands the support of security architecture so that the associated system can continuously assess and mitigate risks intelligently. It is required to verify the efficiency of access control of financial system in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, non-repudiation and data integrity. For any secure service, the system should ask the identity and authentication of one or more agents involved in a transaction. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After the identification and authentication, the system should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication.

5. STRATEGY

Strategy Analytics

Agents: **System analysts, business analysts, technology management consultants;**
Strategic moves :

- **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements : scope, system, structure, security, strategy, staff-resources, skill-style-support;**
- **Define a set of financial security goals and emerging technologies accordingly.**
- **Do SWOT analysis: strength, weakness, opportunities and threats of financial security technologies.**
- **Fair and rational business model innovation**
  - **Who are the customers?**
  - **What should be the offering of products and services?**
  - **What do the customers value?**
  - **What is the rational revenue stream?**
  - **How to deliver values to the customers at rational cost?**

- **Do technology life-cycle analysis on 'S' curve : presently at emergence phase of 'S' curve.**
- **Explore technology innovation-adoption-diffusion strategy.**
- **Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.**
- **Adopt '4E' approach for the implementation of financial security globally : Envision, Explore, Exercise and Extend.**

Dr. Ramaswamy is analyzing the strategy for the innovation, adoption and diffusion of financial security technologies. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of top innovations related to financial security today. In the first decade of the 21 Century, financial security technologies were applicable to banking and trading services. Today, the scope of the same has been getting explored in miscellaneous emerging financial services such as financial literacy and education, retail banking, investment to crypto-currencies. In 2008, global investment into Fintech sector was around $900 million and was $27 billion in 2017. Fintech is a flourishing market due to various factors :

(a) Internet and mobile revolution : smartphone penetration surge from 53% in 2014 to 64% in 2018; the number of internet users has been rising from 481 million in December'2017 to 500 million in June'2018; the number of cheap and affordable smartphone users have been rising from 199 million in 2015 to 378 million in 2018.

(b) almostt 40% of the population do not have bank account and over 80% of money transactions are made in cash.

(c) Fintech funding was 21.47% of total startup funding rounds across every market during the first quarter of 2018 and raised over $251 million of funding. Fintech is a startup trend is upsetting the structured format of traditional financial companies such as banks, mobile payments, money transfers and asset management. The worth of Fintech market is expected to double in 2020.

SWOT Analysis **: It is rational to evaluate strength, weakness, opportunities and threats of this innovation. There may be major and minor strengths and weaknesses. Strength indicates positive aspects, benefits and advantages of a strategic option. Weakness indicates negative aspects, limitations and disadvantages of that option. Opportunities indicate the areas of growth of market and industries from the perspective of profit. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses. Financial technologies touche technology, business, and government. Financial technologies have been evolving over the past several decades, there are various types of technological challenges such as risk of cyber attacks, money laundering, information security and privacy and trust in digital currency. Government should play the role of regulator protecting markets and consumers and promoting the innovation, adoption and diffusion of financial technologies globally.**

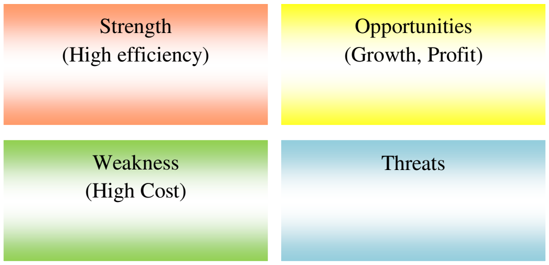


Figure 8.1 : SWOT Analysis

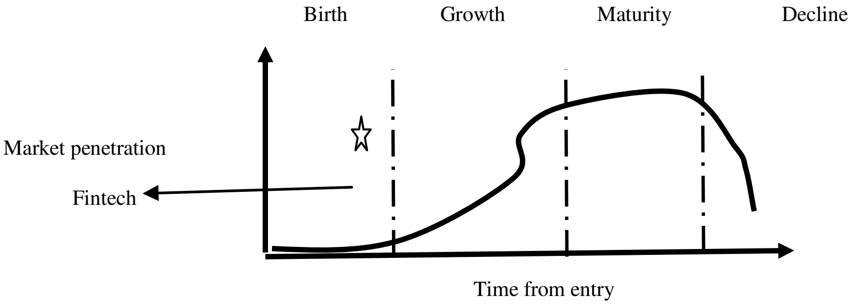


Figure 8.2 : Technology life–cycle analysis of Financial security technologies

Financial security technology life-cycle analysis: Deep analytics evaluate and explores top technological innovations in terms of technology life-cycle, technology trajectory, S-curve, technology diffusion and dominant design. No element in this universe exists eternally. Similarly, each technology emerges, grows to some level of maturity and then declines and eventually expires, At present, most of financial security innovations exists at emerging or birth phase of S-curve as per perception; some are growing at fast pace.

6. STAFF-RESOURCES

Staff-resources Analytics

do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- **Man (human capital management [scientists, business analysts, system analysts, project managers], talent acquisition, talent retention, training, reward and recognition);**
- **Machine (computer hardware, software, internet);**
- **Material (Financial data);**
- **Method (process innovation);**
- **Money (optimal fund allocation, project management, resource allocation, resource distribution).**

Dr. Richardson is analyzing the need of staff-resources in terms of 5M (man, machine, material, method and money) for the innovation of financial technologies. In this connection, human capital should be considered as a strategic asset and a sustainable resource of technological innovation. Talent management demands the skills of human resources for the innovation of financial security technologies. 'Man' explores various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training and performance evaluation. 'Machine' indicates the basic need of computer hardware, software and internet. 'Machine' analyzes various aspects of digital technologies for banking, insurance and financial services such as hardware, software and networking schema. 'Material' analyzes planning of essential resources such as mobile phones, tablets, desktops and laptops to be used for financial operation. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure associated with financial corporations. Finally, 'money' highlights optimal fund allocation for innovation, adoption and diffusion of financial technologies.

It is crucial to analyze the dynamics of this technological innovation in terms of sources of innovation and roles of individuals and organizations, government and collaborative networks; various types of resources are required for effective technological evolution and diffusion. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation and commitment. Innovation demands the motivation and commitment of creative people. The innovation needs useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. A cooperative and collaborative environment must recognize and reward creative talent in time. Organizational creativity is associated with several critical factors such as human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy and organization structure.

7. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- ***Skill*****: technical, financial management, digital technology, information system, legal, corporate governance;**
- ***Style*****: leadership, shared vision, goal setting, intelligent communication protocol, risk assessment and mitigation;**
- ***Support* : proactive, preventive and reactive support.**

Dr. Shi and Dr. Sarapova are exploring skill-style-support necessary for the innovation of financial security technologies. The workforce involved in innovation are expected to develop different types of skills in banking, financial services, regulatory compliance and digital governance. They should be creative in

development of financial security technologies. The diffusion of new technological innovation depends on the skills and capabilities of the human talent. The workforce are expected to develop different types of skills in financial analysis, business analytics, big data analytics, digital technologies (e.g. information and communication technologies, web technology, computer science), system administration and system maintenance. The workforce should develop skills through effective knowledge management programmes. An effective knowledge management system supports creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way.

The system administrators must have leadership skills in smart thinking, communication, coordination and change management. The diffusion of financial security demands the support of smart leadership style; The style is basically the quality of leadership; great leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. What should be the innovation model for effective diffusion of financial security technologies? Is it possible to adopt K-A-B-C-D-E-T-F model? The diffusion of innovation needs the support of great leadership style. They are expected to have leadership skills in smart thinking, communication, coordination and change management. Top management must tackle the complexity of system implementation by developing a dedicated project team, a right mix of committed resources and talents like technical and business experts.

FURTHER READING

- **P.Harker. 2017. Fintech: revolution or evolution. April, USA.**
- **N. S. Sachchidanand Singh. Big data analytics. International Conference on Communication, Information & Computing Technology (ICCICT), pp. 1-4, 2012.**
- **R. Verma and S. R. Mani, Use of big data technologies in capital markets. April, 2014.**
- **M. Peat. Big data in finance. In Finance: The Magazine for Finsia Members, vol. 127, no. 1, pp. 34–36, 2013.**
- **H. Markowitz, Portfolio selection. The Journal of Finance, vol. 7, no. 1, pp. 77–91, 1952.**
- **H.-H. Chen. Stock selection using data envelopment analysis. Industrial Management and Data Systems, vol. 108, no. 9, pp. 1255–1268, 2008.**
- **N. Koochakzadeh, A heuristic stock portfolio optimization approach based on data mining techniques. PhD thesis, Department of Computer Science, University of Calgary, March 2013.**
- **T. Ware. Adaptive statistical evaluation tools for equity ranking models. Canadian Industrial Problem Solving Workshops (Calgary, Canada, May 15-19, 2005),2005.**
- **V.Sharma, B.Pandey and V.Kumar. Importance of big data in financial fraud detection. International Journal Automation and Logistics. Volume 2, No. 4, 2016.**
- **Chintalapati, S.S. and Jyotsna, G. 2013. Application of data mining techniques for financial accounting fraud detection scheme. International**

Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 11, pp.717–724.

- **Clifton, P. et al. 2010. A comprehensive survey of data mining-based fraud detection research. International Conference on Intelligent Computation Technology and Automation, Vol. 1, pp.50–53.**
- **H.Cai et al. China's land market auction evidence of corruption. NBER working paper 15067, June 2009. http://www.nber.org/papers/w15067**

Quiz

1. Please analyze following case studies, assess the risks of financial security and suggest suitable technological solutions.

Fraud detection on GST collection

Agents: Business analyst, Auditor, Buying agents, Selling agents;

Objectives : Fraud detection on tax (GST) collection;

- **Life science / pharmaceuticals**
- **Retail**
- **Consumer goods**

Constraints:

- **GST collection and implementation mechanism,**
- **Availability of information and communication infrastructure, ;**

System : Analytics, Web enabled ERP & SCM system;

Input : Transactional data (e.g. sales, invoice), inventory data, price;

Procedure:

- **Collect sales transactions data;**
- **Audit sales invoices or bills: Price, GST, Discount;**
- **Verify authentication, authorization, correct identification, fairness, correctness, transparency and accountability in sales transactions;**
- **Collect feedback of the buying agents on quality of products.**

Output :

- **Loss in tax collection;**
- **Detect fraudulent transactions;**
- **Detect sales and distribution of fake drugs / poor quality medicines;**

Problem 1 : Analytics on fraud detection against GST collection in life-science / pharmaceutical industry;

Research methodology: Primary data analysis; data collected through interviewing a patient;

Observations: Malicious Business models are promoting innovation, production, sales and distribution of fake drugs (with vague compositions) causing serious side effects and flawed medical devices today: is it not medical ragging or bioterrorism? Following observations, feedback and experience are furnished regarding possible side effects and ineffectiveness of following few medicines prescribed by an authorized doctor for the treatment of diabetic problem and pain in swollen

scrotum as a result of side effects. Is it really medical ragging or bio-terrorism or sybil attack in sales and distribution of healthcare sector?

SL No.	Medicine	GST Details	Remarks
1	Tenelife-M	Bill given without giving GST details	Discount : 10%; bill given, no GST mentioned in the bill from medicine shop 1; no clarity in prescription
2	Icobal-Forte	No bill given	Discount : 5%; no bill given from medicine shop 2
3	Dolowin	Not known	Given at free of cost at polyclinic; no idea of GST
4	Clavimox 625	No bill given	Discount : 5%; no bill given no bill given from medicine shop 2; no clarity in prescription due to bad hand writing
5	DOTKLOR	Not applicable	Free sample given at free of cost at polyclinic

Table 8.1 : Primary data used for fraud detection

GST collection details against medicines prescribed :

- **Tenelife-M (Teneligipin 20 mg and Metformin Hydrochloride 500 mg.); Discount : 10%; bill given, no GST mentioned in the bill from medicine shop 1;**
- **Icobal-Forte : Discount : 5%; no bill given from medicine shop 2;**
- **Dolowin : Given at free of cost at polyclinic; no idea of GST**
- **Clavimox 625 : Discount : 5%; no bill given from medicine shop 2;**
- **DOTKLOR : Free sample given at free of cost at polyclinic.**

Note : The name of doctor, polyclinic and medicine retail outlets, location and details of bills are private data.

Feedback after consuming aforesaid medicines:

- **No relief of pain**
- **No reduction in blood sugar level**
- **Possible infection in urinary bladder and natural activities**
- **Diabetic gangrene (as diagnosed)**
- **Physical weakness and deterioration of health conditions of the patient.**

Is it not essential in taking necessary corrective actions and precautions in drug discovery and irrational mechanical innovation from the perspectives of sustainable life-science, biotechnology and pharmacy in future ignoring economic pressure in healthcare sector. It is a critical issue of business modeling and system dynamics and Corporate Social Responsibilities (CSR) in formulation of stressless public policy.

Recommended Mechanism Of GST Collection

- **Adoption of information system for correct billing with detailed computation of GST and discounts;**
    - **Use computers: desktops / laptops**
    - **Use tablets**
    - **Use smart phones**
- **Production of valid prescriptions of doctors essential with clarity (e.g. fairness, correctness, completeness)**
    - **Mobile messages**
    - **Exception :**
        - **Emergency cases (e.g. strokes) : Self declaration by the patients or their relatives through letters;**
        - **Critical drugs (e.g. sleeping pills, pain killers) : Self declaration by the patients or their relatives through letters;**
- **Audit of fraudulent transactions and corruptions, use of fake drugs**
- **Real time Inventory control through CPFR (Collaborative planning, forecasting and replenishment), S&OP**

Quiz

- **What is the scope of financial security technology?**
- **What is the dominant design of these technologies?**
- **What are the basic elements of the system architecture?**
- **What do you mean by technology security? How can You verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis and SWOT analysis of online and offline technologies?**
- **How to manage resources for innovation project of these technologies**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How do You manage financial security technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**

SESSION 9: SOCIAL SECURITY - SOCIAL ENGINEERING, CANCER OF MIND, INFORMATION, MEDIA AND ENTERTAINMENT TECHNOLOGIES

Event : **Technology for humanity and global security summit**
Venue: **Social security hall, Technology park : Sanada**
Time Schedule : **3 p.m. – 6 p.m. , 17.8.2020**
Agents : **Representatives of various global organizations (Global nations, global childcare organization, global peace organization, global health organization, global financial organization, global economic forum), Technology management experts from science and technology forums, Social engineers, Social scientists, representatives and ministers from the departments of child, women and family welfare of developed, developing and underdeveloped countries, CEOs of social media corporations, business development consultants of information, media and entertainments sectors, reprentatives from NGOs.**
Topic of discussion and key focus areas: **social security, social networking, social engineering, cancer of mind.**
Keynote speakers: **Prof. S. Nelson, Prof. Nancy Robson, Prof. R. Subramanium, Prof. P. Ronaldinho, Dr. Gremy Smith.**

1. SCOPE

Scope Analytics
Agents: **Social scientists, system analysts, business analysts;**
Moves : **Critical success factors analysis, Requirements management;**
Social security parameters: **Define a set of sustainable development goals for social security.**

- ✪ **religious and cultural security, gender equality, child security, women's empowerment, safety of senior citizen, peace, justice, partnership, job security (decent work) and regulatory compliance through strong institutions.**
- ✪ **Poverty control of refugees and migrants /* scope analytics, chapter 1*/**
- ✪ **Safety against war, act of terrorism, crime, bioterrorism and natural disaster;**
- ✪ **Healthcare, ageing population, technological transition, higher public expectations, employment of young workforce, labour markets and digital economy, protection of migrant workforce, inequalities and discrimination, new risks, shocks and extreme events;**

Prof. Nancy Robson has started the session highlighting the aforesaid scope analytics. She is giving a multidimensional view of social security in terms of religious and cultural security, gender equality, child security, women's empowerment, safety of senior citizen, peace, justice, partnership, job security (decent work) and regulatory compliance through strong institutions. The key focus areas of this session is the emerging digital technologies such as social networking,

social engineering and stress management and also evolution of social security technologies through deep analytics. The expert panel have planned to analyze a case study on cancer of mind at the end of the session. Social security is deeply related to human psychological problem, mental stress and depression of the kids, boys, girls, young people, men and women and senior citizen.

2. SYSTEM

System Analytics

***Agents*: System analysts, business analysts, Social scientists;**
***Moves* : Requirements engineering, system design, coding, prototype testing, erection, installation, testing, commissioning**
***Emerging technologies*: Innovate a set of emerging technologies based on social security. /* Refer to scope analytics, section 1 */**

- ✪ **Social networking (secure access control, private encrypted message communication, private publishing of image, video, data streaming)**
- ✪ **Social security :**
  - ▪ **Child security: Technologies related to sports and games**
    - ▪ **Indoor games (toys, caroms, ludos, table tennis, chess)**
    - ▪ **Outdoor games (football, cricket, hockey, volleyball, basketball, rugby, tennis, badminton, baseball, cycling, athletics)**
    - ▪ **Yoga and physical exercises (Tools used in gymnasiums and health fitness clubs)**
    - ▪ **Meditation**
    - ▪ **Social media , webmail, e-chat;**
  - ▪ **Women's empowerment : social media;**
  - ▪ **Gender equality : social media;**
  - ▪ **Safety of senior citizen : mechatronics, mechanical, old age home;**
  - ▪ **Religious and cultural security : Broadcast communication of divine religious and cultural rituals and activities at temples, mosques, churches etc. using virtual reality technology;**
  - ▪ **Peace : Defense, CCTVs, Webcams, Drones for surveillance operation by police force, army, fire brigade and disaster management workforce;**
  - ▪ **Justice : AI and logic based automated legal system, case based reasoning, digital governance;**
  - ▪ **Partnership : strategic alliance, collaborative intelligence;**
  - ▪ **Job security : decent work, workplace safety, HR information system;**
  - ▪ **regulatory compliance through strong institutions : Regtech analytics**
- ✪ **Poverty control of refugees and migrants /* Refer chapter 1*/**
- ✪ **Safety against war, act of terrorism, crime, bioterrorism and natural disaster /* Refer chapter 2.**
- ✪ **Technologies for education and financial security**

- **Healthcare, ageing population, higher public expectations : Health insurance system, retirement planning & pension system,**
- **Technological transition, inequalities and discrimination, new risks, shocks and extreme events: Strategic risk analytics;**
- **Employment of young workforce, labour markets and digital economy, protection of migrant workforce : Human resource management system;**

Prof. Nelson, Prof. Ronaldinho and Dr. Parker are exploring the system associated with the innovation of emerging social security technologies. Social networking is an emerging technology; popular social networking sites have several billion monthly and daily users. It is an online platform which is used to build social networks or social relationships based on similar personal or career interests, activities, backgrounds or real-life connections. Social networking services may have various types of format and number of features such as digital photo and video sharing, posting comments and online blogging. The technology is accessible through various types of popular information and communication tools, desktops, laptops, tablets and smart phones.

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information through various ways such as vishing, phishing, smishing, impersonation, water holing, baiting and quid pro quo. It is essential to develop information security culture. Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. It is an interesting agenda to explore the relationship between organizational culture and information security culture. It is possible to develop information security culture through pre-evaluation, strategic planning, operative planning, implementation and post-evaluation.

3. STRUCTURE

Structure Analytics

***Agents*: System analysts, business analysts;**

***Moves*: Design and configure**

- **Organization structure**
  - **Technology forums**
  - **National level : Government (E-governance model), NGOs, research organizations, ;**
  - **International level : strategic alliance among global organizations (nations, heath, child, peace);**
- **System architecture (topology, modules, nodes, connectivity, layers);**
  - ***Emerging technologies* : Innovate a set of emerging technologies as per the goals of social security;**
  - ***Level 1*: digital technology, information technology, computer science, electrical, electronics, telecommunication, chemical, mechanical, civil engineering;**

- ***Level 2*: Identify fundamental building blocks of information technology:**
    - **computing**
    - **data (data warehouses, big data analytics, performance scorecard)**
    - **networking (web mail)**
    - **security schema**
    - **application (social networking)**
    - **Social networking services (friendship, dating, job search, career growth planning, employment, research, policy making, search for resource**

Prof. Nelson is presenting the basic structure of social security technologies. Social networking services may be structured into various categories: social network services for socializing with existing friends (e.g. Facebook, Twitter) through online distributed computer networks and internet services, networking services used or non-social interpersonal communication on job search, career growth planning and employment, social navigation for helping users to find specific information or resources (e.g. products, services, books, medicines, healthcare, travel, hospitality) and services for researchers and policymakers. Social networking services may be categorized based on age, occupation and religion supported by trusted recommendation system. A social network service usually provides an individual centered service whereas online community services are group centered to maintain and develop new social and professional relationships and to offer opportunities within professional education, curriculum education, and learning, to make new business contacts or keep in touch with previous alumni, co-workers, affiliates and clients. Social networking services provide a virtual space for learners through participation, collaboration, distribution, dispersion of expertise and relatedness. Registered users share and search for knowledge which contributes to informal learning.

Excessive use of social networking may affect the young community such as wasting time, cyber bullying, invasions of privacy, social anxiety, abuses resulting conflicts in relationship management and depression. Blocking and banning of social networking services for the student community may not be a rational solution. The community should be alert of addiction of social media and cyberbullying. Social networking services often share personal data of the users which may be a window into privacy theft.

4. SECURITY

Security Analytics

***Agents*: kids, children, youth, men, women, senior people;**

***Organization* : Security council of global organizations;**

***Social security goals* : healthcare, ageing population, technological transition, higher public expectations, employment of young workforce, labour markets and digital economy, protection of migrant workforce, inequalities and discrimination, new risks, shocks and extreme events;**

***Verification mechanism*: audit *security intelligence* through intelligent *surveillance technologies* (e.g. drones, CCTVs, webcams, smartphones).**

- ***multi-party corruption:* do surveillance through security council of global organization, police, army, detectives, journalists ;**
  - ***Social crimes : Ensure safety f*rom (relationship management problems, superstition, narrow religious outlook, sex, domestic violence, drug and alcohol addiction, addiction of pornographic films and video games, smoking, mental stress, panic, financial crime);**
  - **Safety *from natural disaster/ /* refer chapter 2*/***
  - **Safety from war, bioterrorism and acts of terrorisms**
- ***access control*: verify authentication, authorization, correct identification, privacy, audit confidentiality, data integrity and non-repudiation;**
- **social security policy: verify rationality, fairness, correctness, transparency, accountability, trust and commitment;**
- ***system performance:* verify reliability, consistency, scalability, resiliency, liveness, deadlock freeness, reachability, synchronization, safety;**
- ***malicious attacks*: verify the risk of Sybil, false data injection, shilling: push and pull, denial of service (DoS), fault injection attack;**
- ***web security:* session hijack, phishing, hacking, cross site request forgery, cross site script, broken authentication, improper error handling;**
- **Social engineering : vishing, pretexting vishing, phishing, spear phishing, smishing, impersonation, water holing, baiting, quid pro quo;**

call threat analytics and assess risks of emerging digital technologies (e.g. social networking sites, social media, broadcast communication) :

- **what is corrupted or compromised (agents, computing schema, communication schema, data schema, application schema)? detect type of threat.**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights : how and why did it occur? do cause-effect analysis on performance, sensitivity, trends, exception and alerts.**
- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**

***Output*: security intelligence**

Prof. Roberts and Dr. Gremy Smith are exploring the security of social networking services through a case analysis on cancer of mind, depression and stress management (section 8).. There are various methods of social engineering based on specific attributes of human decision making, cognitive biases or bugs in human hardware. Social engineering can steal confidential data of the users through phones, session hijack, criminal posing or stealing of company secrets. A malicious hacker may contact the target through a social networking site; gains the trust of the target and tries to access sensitive private data. Social engineering relies heavily on various principles of influence such as reciprocity, commitment and consistency, social proof, authority, liking and scarcity. Reciprocity forces people to return a favor. Commitment and consistency forces people to disclose private data.

Authority may force a user to reveal critical strategic information. People are easily persuaded by other people whom they like. Perceived scarcity may generate demand. Vishing or voice phishing is the criminal practice of using social engineering over telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. Phishing is a technique of fraudulently obtaining private information through e-mail. Smishing is use of SMS to lure victims into a specific course of action. Like phishing, it can be clicking on a malicious link or divulging information. Impersonation is pretending to be another person with the goal of gaining access physically to a system. The life-cycle of social engineering goes through information gathering, engaging with victim, attacking and closing interaction.

Pretexting is the act of creating and using an invented scenario to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. Vishing uses a rogue interactive voice response (IVR) system. Spear phishing fraudulently obtains private information by sending highly custom emails to few end users. Water holing is a targeted social engineering strategy that capitalizes on the trust users have in websites they regularly visit. The victim feels safe to do things they would not do in a different situation. Baiting is like the real-world Trojan horse that uses physical media and relies on the curiosity or greed of the victim. Quid pro quo means something for something. In case of tailgating, an attacker, may seek entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access.

The security intelligence of regulatory compliance is a multi-dimensional parameter which should be verified at various levels. The regulatory clauses should be defined and audited by a group of authorized agents correctly and rationally. The scope of social security technologies should be correctly identified; relevant data should be sourced through authenticated channels. The social networking system should preserve confidentiality, privacy and integrity of data. For any critical analysis, the system should ask the identity and authentication of the users. After correct identification and authentication, the system should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task. The agents should be assigned an explicit set of access rights according to role. Privacy is another important issue; the analysts can view only the information according to authorized access rights.

It is also crucial to verify and evaluate various rules and regulatory clauses for social security in terms of fairness, correctness, rationality, transparency, accountability, commitment and trust. It is essential to evaluate the performance of the system in terms of reliability, consistency, and stability. The performance of the system is expected to be consistent and reliable. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that the system should never be in a state in which no progress is possible. The system should be protected from various types of internal and external malicious attacks such as false data injection, Sybil, shilling and denial of service (DoS) attack. The

auditors must assess the threats of such types malicious attacks by adversaries. It is also important to assess the risk of multi-party corruptions on the social security technologies in terms of agents, policy, procedure and protocol. An efficient knowledge based system is expected to monitor the gaps and violations in regulatory compliance in real-time and diagnose any fault just like supervisory control and data acquisition system.

5. STRATEGY

Strategy Analytics

***Agents*: System analysts, business analysts, technology management consultants;**
***Strategic moves* :**

- ✪ **Call deep analytics '7-S' model; explore how to ensure a perfect fit among 7-S elements – scope, system, structure, security, strategy, staff-resources, skill-style-support;**
- ✪ **Define a set of social security goals and emerging technologies accordingly.**
- ✪ **Do SWOT analysis: strength, weakness, opportunities and threats of existing technologies related to e-governance, digital technologies, social networking technologies, police, army, detectives.**
- ✪ **Fair and rational business model innovation associated with entertainment, culture and religious rituals**
  - ▪ **Who are the consumers?**
  - ▪ **What should be the offering of products and services?**
  - ▪ **What do the consumers value?**
  - ▪ **What is the rational revenue stream?**
  - ▪ **How to deliver values to the consumers at rational cost?**
- ✪ **Do technology life-cycle analysis on 'S' curve : presently at growth phase of 'S' curve.**
- ✪ **Explore technology innovation-adoption-diffusion strategy for real-time surveillance system.**
- ✪ **Explore innovation model and knowledge management system for creation, storage, sharing and application of knowledge.**
- ✪ **Adopt '4E' approach for the implementation of social security globally : Envision, Explore, Exercise and Extend.**

Case: Poverty, Intrusion and Enterprise Resource Planning

Prof. Subramanian is exploring the strategy for innovation of emerging technologies to ensure social security Let us look at the problem of poverty of a group of neighboring countries: I, B, P, N, S and C. The ministries of finance and economic affairs, home, defense and foreign affairs of country I are brainstorming how to control poverty, create more job opportunities through business model innovation and countermeasures against environmental pollution. The points of discussion are as follows:

Is poverty really the outcome of luxurious passion and fashion of the economists and public policy makers globally today?

Is it rational to copy the concept of chemical equilibrium into economic equilibrium to maintain the stability of the global economy?

Should the government of country I be indifferent to regulate intrusion, migration and infiltration of the refugees from neighbors (e.g. B, P, N) to control poverty and unemployment being provoked by the wise sayings like tolerance, unity in diversity, collaborative intelligence, humanity, actions against promotion of hate crimes and vote bank politics? What are the risks and countermeasures to avoid economic stress in job market and optimal fair resource distribution in country I today? Is it not essential to adopt a strict immigration policy, citizen amendment bill (CAB), national registry of citizens (NRC) and ERP system to curb the problem of intrusion and poverty?

If more resources are allocated and distributed to the poor people of the society by Govt. of I, there will be more intrusion and infiltration from the neighbors to country I and there will be spiraling effects in poverty statistics. The poor people from the neighboring countries will be attracted to the facilities and opportunities adopted by Govt. of country I. The local people of country I are facing the stress in job market and deprived of fair resource allocation and distribution due to the pressure from the refugees / migrants / infiltrators. A large portion of the resources (e.g. space, land, food, energy, utilities) are captured by the refugees, infiltrators and migrants who are involved in setting up their local colony and culture through strategic alliance. Look at the local people of state W of country I. They are forced to migrate to the other states of country I but ill-treated and forced to come back to W. The recent killing of several laborers in state K of country may be a good example of the problem. The migrants are coming to W. They are setting up their own colony, culture and educational system and running parallel government. The migrants and refugees are involved in bad culture ('apasanskriti') and malicious antisocial activities silently through fake broadcast and false data injection attack; the real contributions are big zero; hate crimes (jatibiddesh) are getting originated through a natural process. The resources are getting consumed by the intruders / migrants / refugees in unregulated manner which will surely create problems of resource planning, allocation and distribution in future. It is the time to think scientifically. The local people of I and state W are at war, helpless, victimized and burdened.

So what should be the solution for the burden of intruders/ infiltrators / migrants for poverty control? The conflict between ERP (Enterprise Resource Planning) and emotional economics is inevitable. An interesting solution may be 'Uniform growth and development for all' through collaboration in neighboring countries and proper rehabilitation of the refugees, intruders and infiltrators in the neighboring country / state through back-propagation mechanism. If more resources are distributed to all the poor people of all neighboring countries (e.g. minimum income) and there is uniform economic development, there will be less intrusion of the refugees towards country I and state W. It may be then easier to tackle the rising problem of poverty and unemployment. Border security force of country I may not be able to tackle the problem of migration and infiltration alone. Country I should help the neighbors

following the policy of collaborative intelligence in various domains such as technology management, public policy for poverty control measures and infrastructure development. The ministry of defense, home, foreign and economic affairs of country I are expected to work with governments of neighboring countries closely and jointly. It is a critical issue of fairness, correctness, transparency, accountability and rationality in enterprise resource planning and supply chain management; it is rational to think from the resource based view of a nation, country and state.

The ministers of the aforesaid ministries are also considering several other issues:

- Is the broadcast communication system in country I (e.g. newspapers, TV, radio channels) captured and compromised by the intruders, infiltrators, migrants and refugees from the neighbors?

- Is it rational to focus on traditional old models of Economics such as Keynes and David Ricardo for poverty control?

- Are the books on poor economics in hard times really written by the great economists or the outcome of the perception based nonfactual readymade immatured confused thoughts of the students / academic community at the college canteens of the academic institutes? Are all data mentioned in the books on poor economics in hard times authentic or readymade?

Is the resource based view of a firm similar to the resource based view of a nation / state / country? What are the negative impacts of unregulated resource consumption by the intruders, refugees, infiltrators and migrants in a country or a state ? Will not there be shortage of resources in future in country I? If there is unlimited increase in consumption by the intruders and refugees; there may be increase in demand for a firm in short run but there will be shortage of resources and economic stress in job market for the local people of a country in long run! The local folks may be forced to struggle for existence. Did the great economists think from the perspective of optimal enterprise resource planning (ERP) and supply chain management (SCM) in their old time? Does country I need critical thinking and deep analytics on HR and business model innovation today; the problem of poverty is not so trivial at all; traditional old models may be dead and obsolete in modern times! An apparently popular solution may be a disaster due to biased, perception based nonfactual readymade immature confused thoughts of the so called intellectuals! It is a question of the security of a country : be it social security or defense. The ministries have decided to focus on technology management i.e. proper innovation, adoption and diffusion of a set of path breaking technologies to fight against poverty, environmental pollution and creating new job opportunities through business model innovation.

6. STAFF-RESOURCES

Staff-resources Analytics

do estimation, planning, capacity utilization, allocation and distribution of '5M' resources.

- Man (human capital management [social scientists, business analysts, system analysts, project managers], talent acquisition, talent retention, training, reward and recognition);
- Machine (computer hardware, software, internet);
- Material (data at social networking sites, toys, tools for sports and games);
- Method (process innovation);
- Money (optimal fund allocation, project management, resource allocation, resource distribution).

Prof. Nancy Robson is analyzing the need of staff-resources in terms of 5M (man, machine, material, method and money) for the innovation of social security technologies. In this connection, human capital should be considered as a strategic asset and a sustainable resource of technological innovation. Talent management demands the skills of human resources for the innovation of social security technologies. 'Man' explores various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training and performance evaluation. 'Machine' indicates the basic need of computer hardware, software and internet. 'Material' is related to toys, equipments and tools used for various types of sports and games. 'Method' explores various aspects of process innovation, intelligent mechanism and procedure for the innovation of social security technologies. Finally, 'money' explores the scope of optimal fund allocation for innovation and diffusion of technologies.

It is crucial to analyze the dynamics of this technological innovation in terms of sources of innovation and roles of individuals and organizations, government and collaborative networks; various resources required for effective technological evolution and diffusion. Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation and commitment. Innovation demands the motivation and commitment of creative people. The innovation needs useful and novel support of creative, skilled, experienced and knowledgeable talent. Creative talent can look at the problems in unconventional ways; can generate new ideas and articulate shared vision through their intellectual abilities, knowledge, novel thinking style, personality, motivation, confidence, commitment and group dynamics. A cooperative and collaborative environment must recognize and reward creative talent in time. Organizational creativity is associated with several critical factors such as human capital management, talent acquisition and retention policy, complex and tacit knowledge management strategy and organization structure.

7. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

- ***Skill*: technical, system admin, management, legal, governance, surveillance, relationship management;**

- ***Style*: leadership, shared vision, goal setting, intelligent communication protocol, risk assessment and mitigation;**
- ***Support* : proactive, preventive and reactive support.**

The expert panel have explored skill-style-support necessary for the innovation of social security technologies. The workforce involved in innovation are expected to develop different types of skills in social networking, social media, social engineering and digital governance. They should be creative in development of social security technologies. The diffusion of new technological innovation depends on the skills and capabilities of the human talent. The system administrators must have leadership skills in smart thinking, communication, coordination and change management. The workforce should develop skills through effective knowledge management programmes. An effective knowledge management system should support creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of social security demands the support of smart leadership style; The style is basically the quality of leadership; great leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. What should be the innovation model for effective diffusion of social security technologies? Is it possible to adopt K-A-B-C-D-E-T-F model?

It is essential to develop information security culture at organization level through pre-evaluation, strategic planning, operative planning, implementation and post-evaluation. Pre-evaluation identifies the awareness of information security within employees through analysis of current security policy. Strategic planning comes up with a better awareness-program with clear targets. Operative planning sets a good security culture based on internal communication, management buy-in, security awareness and training program. The final stage is implementation of information security culture through the commitment of management and employees of the organization.

8. CASE: CANCER OF MIND & SOCIAL SECURITY

The expert panel are analyzing a case on cancer of mind which affects social security seriously. . They have defined and identified major causes of cancer of mind. Cancer of mind is the inability to cope with a perceived or real threat to one's physical, mental, emotional and spiritual well being which results in a series of physiological responses and adaptation. It is human body's physical, mental and classical reaction to circumstances that frightens, confuses, endangers or irritates human agents. It is basically mental tension. If controlled, it may be a friend that strengthens human beings for the next encounter. But, is it really easy to control cancer of mind? It is basically mental tension; it is a feeling of strain and pressure. It is a type of physiological pain.

What are the symptoms and characteristics of cancer of mind: depression, anxiety, anger, irritabilities, restlessness, feeling overwhelmed, unmotivated or unfocused, trouble in sleeping or sleeping too much, racing thoughts and constant worry, problems with memory or concentration and making bad decisions. Cancer of mind

may have negative effects on health: high blood pressure, heart disease,, diabetes, obesity, depression, anxiety, skin problem (acme or eczema) and menstrual problems. It is debatable whether cancer of mind has any positive effects such as boosting brainpower, increase of short term immunity, increase of strength, creativity, motivation of success and developments of the children. Cognitive symptoms may be memory problems, inability to concentrate, poor judgement, seeing negative attitude and constant worrying. The emotional symptoms may be depression and general unhappiness, anxiety, agitation, moodiness, anger or irritability, feeling overwhelmed, lonliness and isolation, internal and external emotional problems. Physical symptoms may be aches and pain, diahorrea, constipation, nausea, dizziness, chest pain, rapid heart rate, loss of sex drive, frequent cold or flue. Behavioral symptoms may be eating more or less, sleeping too much or too little, withdraw from others, drug addiction, smoking, alcoholic addiction, nervous habits, procrastinating or neglecting responsibilities.

The next critical issue is how to identify cancer of mind? There sre several behavioral signs : no time for relaxation or pleasant activities, prone to accidents and forgetfulness, increased reliance on alcohol, smoking, caffeine, recreational or illegal drugs, becoming a workaholic, poor time management, poor standards of works, absenteeism, self negligence, change in appearance and social withdrawal. What are various types of cancer of mind? It is a physical, mental or emotional factor that causes physical or mental tension. It may be internal due to illness or medical surgery or external due to environment, phycological or social factors. It may be anticipatory, situational or encounter. It may be cognitive (e.g. information overloading, guilt, panic, anxiety), acute (single, repeated) or chronic cancer of mind (if acute cancer of mind is not resolved and lasts for long period) or emotional cancer of mind (mental strain, fear, fraustration, sadness, anger, grief). What are the sources of cancer of mind : money or financial troubles, job issues, relationship conflicts, life changes; loss of loved one (spouses, grief, relatives, long daily journey, abuse, insult and physical torture. The expert panel are outlining a mechanism for restricting cancer of mind.

***Agents*: Defender (e.g. human agent, doctor), Attacker (e.g. malicious agent or adversary);**

***Model*: Human mind;**

***Objectives*: cancer prevention at optimal cost;**

***Constraints*: budget or financial constraint, resources, time, knowledge;**

***Input*: Perception of human agent, performance measures of biological system or test data;**

***Strategic moves*: intelligent reasoning, optimal mix of proactive and reactive approaches, rational payment function and budget plan;**

***Revelation principle*: The agents preserve privacy of strategic data;**

- **Defender : The defenders share critical information collaboratively.**
- **Attacker : The adversaries do not reveal the plan of malicious attack, information of targets and weak links in advance.**

***Cancer Prevention Approaches*:**

- **Proactive approach:**

- **Identify targets :**
    - **application schema – human mind;**
    - **networking schema – brain and nervous system;**
    - **computing schema – nerve impulse and release of neurotransmitter;**
    - **data schema – symptoms of abnormal, selfish behavior, narrow outlook, jealousy, negative mechanical robotic thinking, devil's thought, fear of death, anxiety, impatience, restlessness, hyperactive behavior, depression;**
    - **Security schema – auto immunity, hormones, vitamins, minerals, genetic traits;**
- **Threat modeling**
    - **Call threat analytics and assess miscellaneous risk elements :**
        - **change in behavior, physical appearance and personality;**
        - **psycho-oncology disoder;**
        - **Schizophrenia : multiple personalities, severe mental disorder in thinking, perception, emotion, sense of self and violent behavior;**
    - **Estimate demand plan;**
    - **Explore risk mitigation plan : accept / transfer / remove / mitigate risks.**
        - **Vaccination (option to be explored);**
        - **Optimal diet intake to fight against malnutrition;**
        - **Life-style : Avoid smoking, alcohols and drug addiction;**
        - **Stress control through yoga and meditation, deep sleep;**
        - **Listen soft relaxation music during idle time in subconscious mind.**

Reactive approach:

- **adopt sense-and-respond strategy.**
- **assess risks of single or multiple attacks on the mind; analyze performance, sensitivity, trends, exception and alerts.**
    - **what is corrupted or compromised?**
    - **time series analysis : what occurred? what is occuring? what will occur?**
    - **insights : how and why did it occur? do cause-effect analysis.**
    - **recommend : what is the next best action?**
    - **predict: what is the best or worst that can happen?**
- **verify security intelligence of application, computing, networking, security and data schema of human mind.**
    - **Level1: correctness, fairness, accountability, transparency, rationality, trust, commitment;**

        - ♦ **Level 2: authentication, authorization, correct identification, privacy, audit;**
        - ♦ **Level3: safety, reliability, consistency, liveness, deadlock-freeness, reachability, resiliency;**
        - ♦ **Level4: stability, system dynamics, quality of application integration.**
    - **Explore risk mitigation plan.**
        - ♦ **Do medical testing → Data visualization of brain scan;**
        - ♦ **Integrated medicine**
        - ♦ **Psychiatric oncology**
        - ♦ **Behavioral and cognitive therapy**

- **Fight against bad luck: Identify critical risk elements.**
    - ♦ **Genetic disorder**
    - ♦ **Reproductive disorder (personal, hormonal and family history)**
    - ♦ **Occupational exposure**
    - ♦ **Injuries from accidents, war and crime**
    - ♦ **Environmental pollution (e.g. air, sound)**
    - ♦ **Hostile climate, weather and other locational disadvantages, exposure to sunshine**
  - **Develop risk mitigation plan in terms of deaddiction and rehabilitation.**

Payment function:

- ♦ **Select dominant strategy of healthcare investment from the options of reinforcement on the weakest link, experimental treatment, process re-engineering, transformational and renewal.**
- ♦ **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements.**
- ♦ **Trade-off proactive vs. reactive security: assign weights to each approach.**
- ♦ **Allocate healthcare budget in the ratio x:y:z where x: fund for proactive approach, y : fund for reactive approach and z: health insurance premium;**

Output: Prevention plan of cancer of mind

Why cancer of mind is so critical to the student community of the world? The student community faces cancer of mind due to various reasons such as academic pressure, vast courses, different types of courses, information overloading, pressure of activity based learning, completion of assignment based projects within deadline, mental depression due to poor performance in examinations, abuses from teachers, parents, friends and relatives, relationship management problem, financial pressure of education loans, exhaustive effects of long journeys for going to school, pressure of intensive competition, rivalry, panic, jealousy, examination, deadline, pressure of combating paid work and study, difficulty in organizing works, pressure of long hour study, poor time management and out of control debts.. The students may have some common symptoms of cancer of mind : difficulty in sleeping, weight gain

or weight loss, stomach pain, irritability, teeth grinding, panic attacks, headaches and difficulty in concentration. There are some common signs of cancer of mind for the students such as personality change, agitated, withdrawal syndrome, poor self-care, hopelessness. How can the student community manage cancer of mind ? There are various strategies for reducing cancer of mind: physical (yoga, meditation, exercises), morning walk, get more sleep, adopt relaxation techniques such as listening soft instrumental music, talk to near and dear ones, physical activities, avoiding drugs, alcohol, caffeine and smoking, time management, disciplined life-style, intake of nutritious food (e.g vitamins B1, B2,B3,B6,B9,B12, milk, sufficient water, spinach, fruits, vegetables).

***Drug addiction* is a major cause of cancer of mind. There is slight difference between cancer of mind and madness. A human agent suffering from cancer of mind may act selfishly with narrow outlook and malicious business intelligence. But, a mad man generally acts irrationally. Any chemical substance other than food used for the prevention, diagnosis, alleviation, treatment or cure of a disease of human agents or animals is called a *drug* or medicine or therapeutic agent. Drug addiction is the habitual, physiological and psychological dependence on a substance or a practice which is beyond voluntary control of an addict. Addictive drug modifies the biological, psychological and social behavior of the addicted person by stimulating, depressing or distorting the function of their body and mind. Use is basically taking a drug for medical treatment like disorder or injury. Drug abuse is the wrong, improper, injurious and misuse of drugs for non-medical purposes which affects physical and mental health of the drug abuser. They use drugs without the prescription of the doctors secretly; taken frequently and regularly; habituating substances; may affect brain and nervous system and changes behavior; gives temporary pleasure or relief from stress. A doctor prescribes drugs for the treatment of diseases or for the improvement of physical and mental health and the drugs are withdrawn as soon as the desired effect is achieved. Repeated use of some drugs on a periodic or continuous basis may make the body dependent on those drugs, It is *drug dependence*. The drug action is affected by a set of factors such as the form, type, dose, mode of use, period of consumption and susceptibility of the addicted person. The addicted person becomes drug dependent through various stages such as experimental use for curiosity, recreational use, situational use, compulsive use and dependence. The addicted person shows some abnormal symptoms such as poor academic performance, indifference in the duties and responsibilities, change in behavior (e.g. telling lies, violence, unrest), change of physical appearance (e.g. loss of weight, vigor and appetite) and change in personality. There are two types of drug dependence - psychological and physical or neuroadaptation. In case of physical dependence, intake of drugs is essential to maintain physiological equilibrium. In case of psychological dependence, a person believes that the normal state can only be achieved with the action of the drugs.**

There are several critical *causal factors* of drug addiction such as curiosity, the pressure from friends and relatives, high stress, pleasure, temporary relief from mental stress, frustration and depression, poor academic performance, problems in relationship management, job loss, unemployment, desire for more work, looking for a different world, relief from pain, family history, easy availability of drugs and

money and excitement and adventure. Some students take drugs to keep awake the whole night for the preparation of their examinations or to manage high work load or backlog. It is a malpractice and bad habit.

Drugs act on brain and central nervous system. The structural and functional units of nerve cells are neurons; the message passes from one neuron to the other through synapses. Arrival of the nerve impulse causes the release of a chemical neurotransmitter. The drugs act at the synapses. The depressant drugs (e.g. alcohol, narcotics) inhibit the production of neurotransmitter or inactivation of the neurotransmitter more quickly or modify postsynaptic membrane. The stimulants increase the production of neurotransmitter and increase stimulation of the neurons. The general symptoms of drug addiction include excitement, violent nature, exhausted and drowsy appearance, poor concentration, memory loss, loss of interests in works, studies and social life, reduced appetite, vigor and weight and disorder of sleep. Ultimately, it results the cancer of mind of drug addicted people.

The addicts often suffer from the problems of central nervous system, psychosis, Hepatitis-B, AIDS, impotency, chromosal abnormalities and genetic disorder. Many of them have a dull unhappy life. They create problems for their families, neglect duties and may lose jobs. It may deprive a family of basic needs and may result frustration and insecurity of the children. The family members may suffer from physical and psychiatric problems such as headache, anxiety, insomnia and depression. The drug users get drugs from illegal sources encouraging smuggling, criminal activities, bio-terrorism and accidents. The drug addicts are less efficient and unreliable as workers and often lose their job or may not get employment anywhere.

Life-science supply chain is a soft target of bio-terrorism. The drugs and medicines sold through popular distribution channels may be tainted, compromised and mislabeled. It needs strong support of drug quality and security act. The life-science supply chain has developed and produced breakthrough drugs and medicines that enhance the average life span in the world. Unfortunately, when bad things happen in life-science supply chain, the public get hurt. Today's life science supply chain requires an effective *'Drug Quality and Security Act and Standards'* which is able to clarify with transparency the authority, roles and responsibilities of food and drugs administration and consumer protection ministry, regulate pricing of drugs, develop a national track-and-trace system to audit the functions of the life-science supply chain and minimize the risks of contamination, adulteration, diversion or counterfeiting.

It is essential to adopt a set of *good habits* by the students and youth as proactive approach through a value based education system at school and colleges to mitigate the risks of drug abuse.

- **Intelligent reasoning through common sense, logical and analytical mind set;**
- **Be proactive and take responsibility of your life. Avoid bad habits and negative thinking; adopt good habits;**
- **Be dedicated, motivated and committed in learning;**
- **Define vision, mission and goals in life rationally and innovatively;**
- **Control physical and mental stress through yoga, meditation, relaxation music and extracurricular activities;**

- **Be conscious of physical, mental and social health;**
- **Prioritize multiple tasks through proper planning and time management and do the most important things first;**
- **Think win-win; have an everyone-can-win attitude with confidence, patience and perseverance;**
- **Listen to the other people carefully and sincerely. First try to understand and then to be understood;**
- **Promote synergy and collaborative intelligence, work together to achieve more through group dynamics;**
- **Sharpen the saw - renew yourself regularly. Analyze as-is state; find out gap and innovate to-be-state;**
- **Contribute to the society and environment through activities, thoughts and plans.**

There are various strategies to mitigate the risk of drug abuse and drug addiction for reactive approach: deaddiction, childcare, drugs as social stigma, legal punitive action, strict regulatory compliance through effective corporate governance, corporate social responsibilities and good habit development through an effective education system. The physicians should prescribe drugs with responsibility and the pharmacists should not sell drugs without the valid prescriptions of the doctors. The parents should keep a watch and monitor the activities, attitude and behavior of their children. The social workers and policemen should be alert and inform the parents or deaddiction centers in time. In fact, law and the public should take joint responsibility against drug abuse.

***Deaddiction* is basically treatment of drug addiction or withdrawal symptoms of drugs. The major steps of deaddiction include master health check up (e.g. blood test, brain scanning), pharmacotherapy, psychosocial therapy, health restoration, psychological treatment and prevention of relapse. If a drug dependent person fails to get drugs, feels severe physical severe physical and psychological disturbances depending on the type and dosage of drugs. The general treatment of *withdrawal symptoms* of a drug is to replace the drug with a less reinforcing and legally available drug that can be gradually eliminated with decreasing doses. It is Pharmacotherapy. For the drug combination addiction, it is required to withdraw one drug at a time and maintain the others. After the withdrawal symptom subsides, psychological treatment persists and cause craving for the drugs. At this stage, the drug addicts need the moral support of their parents, relatives and friends. They may need the treatment at rehabilitation centers; it is a long term treatment requiring behavioral training of the patients. *Rehabilitation* involves the psychological and social therapy in the form of counseling by relatives, friends and physicians in a sympathetic manner. The patients should learn the ill effects of drug addiction through Psychosocial therapy. The patient also needs supportive measures such as administration of vitamins, proper nutrition, restoration of electrolytic balance and proper hydration. Vitamin C checks the rise of the level of cAMP in human brain. The patient may also need Psychological treatment. Finally, *readdiction* may occur; many addicts restart taking drugs after deaddiction. They should be watched by their near and dear ones.**

It is an interesting agenda to identify various stages and models of cancer of mind with the support of human mind, physiology, stimulus, response, transaction, interaction, pressure-environment fit concept. There are various stages of cancer of mind such as alarm, resistance, exhaustion, fight or flight, damage control, recovery, adaptation and burnout. It is possible to diagnose cancer of mind through a set of common symptoms such as anxiety, panic, workload, pressure, hassle and hurry, irritability and moodiness, physical symptoms (e.g. chest pain, headache, stomach upset) and sleeping disorder. Cancer of mind is a biological response to environmental condition, body's method of reacting to threat, challenge, physical or psychological barriers. It may be a stimulus and demands response, adjustment or adaptation. It is often experienced when a human agent perceives that demand exceeds personal and social resources the individual is able to mobilize. It is a collection of physiological changes that occur when one forces a perceived threat. Individuals behavior is determined by the interaction between individuals. in two directions. It is the degree of fit or match between human agent and his / her workplace environment and other members of an organization..

What are the causes and symptoms of cancer of mind : personal, organizational and environmental. Personal causes of cancer of mind may be personal life style (smoking, alcohol addiction, drug addiction), indisciplined life style / Bohemian life style), negative attitude, violent behavior, loss of control (fear, anger, panic, grief), desperate narrow outlook, superstition, lack of human feelings (love, affection, respect), mechanical, robotic and materialistic outlook, too much ambitious, lack of focus and concentration, lack of confidence, hesitation to take challenges, no goal in life, random aspiration and reservation point and preferential thresholds, intense competition and comparison with others. Work stress is a very important factor - unhappy in job, no job satisfaction, having a heavy workload, too much responsibilities, working long hours, poor management, unclear expectation of work, no management of objectives, no target, no goal, working under dangerous conditions, insecurity of career growth, risk of termination, dull corporate communication, failure in project management, discrimination or harassment at work all these factors may result cancer of minf of working professionals. There are other causal factors of cancer of mind : death of spouse, near and dear ones, divorce, loss of job, increase in financial obligation, getting married, moving to new house, chronic illness or injury, emotional problems (depression, anxiety, anger, grief, guilt, low self esteem, care of senior or sick family members and traumatic event (natural disaster, theft, rape, domestic violence). The environmental factors may be fear and uncertainty, bad attitude and perception, unrealistic expectation, change in life, major changes in life (work or school), relationship difficulties, financial problems, being too easy, children and family. The internal environmental factors may be pessimism, inability to accept uncertainty, rigid thinking, lack of flexibility, negative self talk, unrealistic expectation, perfectionism, all-or-nothing attitude. Major events have negative impact on mind such as death of a spouse, divorce, marriage separation, imprisonment, death of near and dear ones and close family members, injury or illness, marriage, job loss, marriage reconciliation and retirement. The exper panel is not sure whether this problem can help one to accomplish tasks more efficiently; can boost memory,. It is a vital warning system

producing fight-or-fight response when the brain perceives mental stress, it starts flooding the body with cortisol.

What are the consequences of cancer of mind? It may have effects on behavior and personality (e.g. anger, anxiety, panic, bad temper, fear, tired, boring, frustration, hopelessness, sadness, grief, lack of self confidence, lack of self respect), high blood pressure, heart diseases, diabetes, obesity, depression, anxiety, skinn problem, menstruation problem. It may have negative effects on performance such as bad performance, low productivity, increased mistakes in works, increased rejection level, loss of focus, no objectives, no target, no goal, loss of goal, random walk in life, increased time and cost, quality problems, quality of services and making bad decisions. It may affect the performance of an organization in terms of reduced revenue, reduced profit, increased cost, low productivity, poor performance, quality problems and increased cost.

What are the strategies to mitigate the risk of cancer of mind ? The healthy strategies include yoga, meditation, physical exercises, get more sleep, relaxation , listening soft instruemental music, watching TV, chat and talk to near and dear ones, intake of water and nutritious food such as balanced food (milk), fruits, vegetables, vitamins (A,B,C,D,E,K), protein (e.g. fish, meat, egg). Unhealthy strategies include avoiding drug addiction, smoking, alcohol, stress free life-style, be happy and calm. A sick person should follow regular physical exercises, connect to the others, building stronger and more satisfying connections, engaging senses (eye, ear,nose, tongue and skin) for sight, sound, taste, smell, touch and movement, learn to relax, eat a healthy diet; get rest, feeling tired can increase stress by causing one to think irrationally; should get recovery from job loss and unemployment.

The factors that influence cancer of mind include tolerance levels, support network, your sense of control, individual attitude and outlook, ability to deal with emotion, knowledge and preparation. Peer group and social support from near and dear ones, friends, relatives. A strong network of supportive friends and family members free of competition, jealousy, rivalry, hate, frank and free exchange of information, experience, chat and gossip, trust, commitment, motivation, spiritual, be happy – all are important to counter cancer of mind. Another important move is happiness and well being (be happy with positive attitude, job satisfaction, contributing to society, spiritual outlook, do not be too materialistic, donation, religious and cultural outlook, rational setting of individual goal in terms of aspiration point, reservation point and preferential thresholds). Another important factor is workplace environment; excessive workload can interfere individual productivity and performance, may have bad impact on physical and emotional health, affecting personal relationships and home life. Job satisfaction with personal job profile, adaptation, adjustment, ambition, career planning, setting goal of life, positive attitude and mindset – all are important factors to fight against cancer of mind. Each organization needs the support of an effective human resources management system. Is it possible to innovate technologies (e.g. AI techniques, digital, chemical, antidepressants drugs having no side effects) to mitigate the risk of cancer of mind?

FURTHER READING

1. C.E. Alchourrón, Logic of norms and logic of normative propositions, Log. Anal. 12 (1969) 242–268.
2. V. Aleven, Teaching case-based argumentation through a model and examples, PhD dissertation, University of Pittsburgh, 1997.
3. International Social Security Association.
4. S.K.Chaturvedi. 2012. Psychiatric oncology: cancer in mind. Indian Journal Psychiatry. Apr-Jun; 54(2): 111–118.

Quiz

- **What is the scope of social security technology?**
- **What is the dominant design of these technologies?**
- **What are the basic elements of the system architecture?**
- **What do you mean by technology security? How can You verify the security intelligence?**
- **What are the strategic moves of technology innovation, adoption and diffusion? What is the outcome of technology life-cycle analysis and SWOT analysis of online and offline technologies?**
- **How to manage resources for innovation project of these technologies**
- **What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation?**
- **How do You manage social security technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
- **What is cancer of mind ? How is it associated with social security? What are the symptoms and effects of cancer of mind? What are the countermeasures? Can you innovate any AI technologies and HRS to mitigate the risk of cancer of mind?**

SESSION 10: EMERGING DIGITAL TECHNOLOGIES for HUMANITY – INFORMATION & COMMUNICATION SECURITY

Abstract:
Event **: Technology for humanity and global security summit**
Venue: **Information and communication security hall, Technology park : Sanada**
Time Schedule **: 1 p.m.. – 6 p.m. , 17.8.2020**
Agents **: Representatives of various global organizations, Technology management experts from science and technology forums, engineers, scientists, representatives and ministers from the departments of information and communication technologies of developed, developing and underdeveloped countries, CEOs of digital technology corporations, business development consultants.**
Topic of discussion and key focus areas **: Digital technologies, information, media and entertainment**
Keynote speakers **: Prof. Parker Smith, Prof. Pearson, Prof. Kamal Kumar, Prof. Simon Watson, Dr. Aziz, Dr. Henry Plank**

1. SCOPE

Scope Analytics
Explore a set of digital technologies for sustainable development goals.

- **Poverty control : Food security (zero hunger), Home security (disaster proof nano-housing schema), Garments and consumer goods security, Education security, Healthcare security (good health, well being, family planning, population control), Financial security (banking, financial services, tax, insurance, retirement planning, stock and derivative trading, economic growth), Energy security (clean and affordable renewable energy), Utilities security (clean water and sanitaion, gas, computing, internet, telecom), Communication security (internet, broadcast, satellite communication), Logistics security (travel, hospitalities, surface, water, rail, water, EVs and hybrid vehicles), Information, media and entertainment security;**
- **Social security (HR security, decent work, religious and cultural security, gender equality, child security, women's empowerment, peace, justice, partnership, regulatory compliance, strong institutions)**
- **Natural disaster security (climate change, flood, drought, storm, cyclone, earthquake, volcano, snowfall, rainfall, fire, bushfire, global warming, heat wave, epidemic, astronomical hazards) (attack of wild animals, insects, paste); artificial disaster security (defense, war, act of terrorism, bioterrorism)**
- **Responsible consumption and production (Enterprise Resource Planning, Supply Chain Management)**
- **Industry, innovation and infrastructure (smart cities, smart villages)**
- **Life on land (environmental pollution, conservation of resources and forest, population control)**

- **Life below water (marine life, water pollution, global warming, oil leakage, nuclear explosion)**

***Emerging innovative digital technologies*:**

- ***Communication technology:* Satellite communication, mobile communication, broadcast communication, Sensor, global positioning system (GPS), Secure adaptive filter, RFID, IoT, IIoT, cloud computing, cloud streaming, edge computing;**
- ***Information technology:* Information security intelligence analytics, adaptive security, dynamic data protection, cyber security, crash proof code, self healing smart grid; applied AI and machine learning : Deep learning, Robotics, Soft computing; Analytics – Deep analytics, Predictive analytics, Collaborative analytics; virtual and augmented reality, Digital twins, solar computing, Quantum computing, pervasive computing, wearable computing, Ray tracing.**

Prof. Parker Smith and Prof. Pearson have started the session by exploring the scope of emerging digital technologies. With the significant advancement of information and communication technology, computing is perceived to be used as the next utility after water, electricity, gas and telecommunication. This session explores the classification of emerging digital technology through scope analytics. Digital technology can be classified into communication and information technologies. The scope of emerging communication technology is explored in terms of adaptive secure filters in adversarial environment, cloud computing, cloud streaming, cloud analytics, Internet of Things (IoT), Industrial IoT, Edge computing, next generation wireless and mobile communication (e.g.4G,5G,6G,7G,8G), broadcast and satellite communication, RFID and sensor networks. The scope of information technology is explored in terms of adaptive security, dynamic data protection, cyber security, crash proof code; applied AI and machine learning, soft computing, deep learning, robotics; deep analytics, predictive analytics, collaborative analytics, virtual and augmented reality, digital twins, solar computing, pervasive computing, wearable computing, secure multi-party quantum computing and ray tracing. This work also evaluates emerging digital technology in terms of system, structure, security, strategy, staff-resources and skill-style-support. Specifically, the technologies of adaptive security, dynamic data protection, solar computing, secure adaptive filters in adversarial environment and secure multi-party quantum computation have been evaluated in depth. The scope of deep analytics and deep learning have been outlined in sessions 1. Emerging digital technologies are useful in various application domains such as education, healthcare, information, media and entertainment, e-governance, manufacturing, retail, logistics, insurance, banking and financial services and development of smart cities and smart villages. Is it possible to apply digital technologies rationally and intelligently for the education of Dyslexia students by reducing their mental stress, information overloading and improving motivation, trust and commitment of the academic communities?

Figure 8.1 shows the classification of emerging digital technology. This is an interesting example of technology association. Level 1 shows the classification of digital technology. Level 2 shows the technology association of various types of

communication technologies such as cloud computing, cloud streaming, cloud analytics, IoT and IIoT. It is possible to explore the scope of digital technology through Business Process Reengineering (BPR) approach (analyze as-is process and related IS, identify gaps and risks of as-is processes and IS and design to-be processes and system); top-down approach, critical success factor (CSF) analysis based on business objectives, constraints and requirements engineering, value chain analysis, bottom-up approach and inside-outside approach. One of the contributions of this session is scope analytics of emerging digital technology in figure 8.1. The scope analytics shows a set of information and communication technologies; among which the concepts of deep analytics, solar computing and adaptive security are unique.

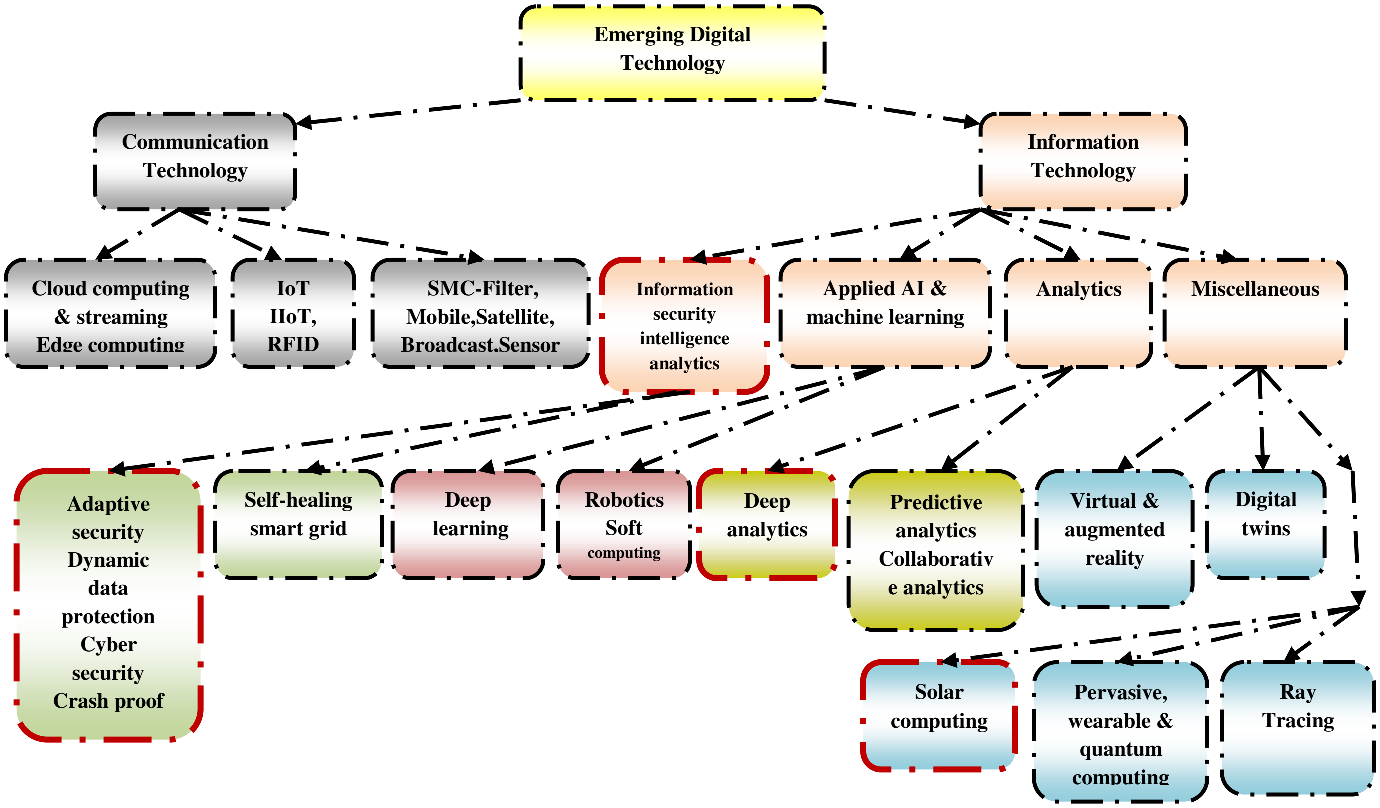

Emerging Digital Technology
Communication Technology
Information Technology
Cloud computing & streaming Edge computing
IoT IIoT, RFID
SMC-Filter, Mobile,Satellite, Broadcast,Sensor
Information security intelligence analytics
Applied AI & machine learning
Analytics
Miscellaneous
Adaptive security Dynamic data protection Cyber security Crash proof
Self-healing smart grid
Deep learning
Robotics Soft computing
Deep analytics
Predictive analytics Collaborative analytics
Virtual & augmented reality
Digital twins
Solar computing
Pervasive, wearable & quantum computing
Ray Tracing

Figure 10.1 : Emerging Digital Technology Classification

Communication Technology **: The scope of emerging communication technology may be explored in terms of cloud computing, cloud streaming, cloud analytics, Internet of Things (IoT), Industrial IoT and Edge computing next generation wireless and mobile communication, broadcast communication, satellite communication, RFID and sensor networks. The wireless technology is going through an evolution of a set of generations (1G→2G→3G→4G→5G→G→7G→8G). This session analyzes the technology of 5G, 6G, 7G, cloud computing, streaming and analytics and edge computing.**

This section performs *SWOT analysis* on the emerging 5G-6G-7G-8G wireless technologies. *5G* is the fifth generation wireless technology for digital cellular

networks with wide deployment in 2019. The frequency spectrum of 5G is classified as millimeter waves, mid band and low band. Low band uses a similar frequency range as 4G. 5G millimeter wave is the fastest having actual speeds 1–2 Gbit/s down. Frequencies are above 24 GHz reaching up to 72 GHz, above lower boundary of extremely high frequency band. 5G mid-band is the most widely deployed in over 20 networks; speed in a 100 MHz wide band is 100–400 Mbit/s down. 5G low-band offers similar capacity to advanced 4G; latencies between 25 -35 milliseconds. 5G networks are digital cellular networks in which the covered service area covered is divided into *cells*. Analog signals (e.g. sounds, images) are digitized by an analog to digital converter and transmitted as a stream of bits. All 5G wireless devices in a cell communicate by radio waves with a local antenna array and low power automated transceiver in the cell, The local antennas are connected with telephone network and Internet through a high bandwidth optical fiber or wireless backhaul connection. A mobile device crossing from one cell to another is automatically hands off seamlessly to the new cell.

***6G (sixth generation)* is the successor to 5G cellular technology; 6G networks are expected to use higher frequencies, higher capacity and much lower latency than 5G networks. 6G is a wireless technology that is beyond 5G. China has officially launched R&D works for 6G mobile networks. It would be about a decade before 6G comes along, NTTDoCoMo has presented the evolution of wireless technology from 3G in 2000s, 4G in 2010, 5G in 2020 and it is reasonable to expect 6G in 2030. It is not exactly known how fast 6G will be yet; it may be governed by the standards of International Telecommunication Union (ITU). If everything connects together using 5G, 6G with higher data speeds and lower latency makes instant device-to-device connection possible in various application such as autonomous cars, drones and smart cities, integration of our brains with computers and greatly improved touch control systems. 7G is the next generation communication technology. It is being adopted in Norway, China, Japan and other developed countries of the world. In Norway, Internet speed is fastest. Utilizing superior design and technology, 7G Network is expected to deliver millions of calls reliably every day,**

Let us exercise *technology analysis* of 5G. The air interface defined by 3GPP for 5G is known as New Radio (NR), and the specification is subdivided into two frequency bands - FR1 (below 6 GHz) and FR2 (mmWave) each with different capabilities. The next issue is frequency range 1 (< 6 GHz); maximum channel bandwidth defined for FR1 is 100 MHz, the most widely band is around 3.5 GHz. For frequency range 2 (> 24 GHz), minimum channel bandwidth defined for FR2 is 50 MHz and the maximum is 400 MHz, From the perspective of *performance analysis;* 5G speed is expected to range from ~50Mbit/s to over 2Gbit/s even 100Gbit/s, 100x faster than 4G. The fastest 5G, known as mmWave, delivers speeds up to and over 2Gbit/s. The latency of 5G is 8 - 12 milliseconds. It is governed by International Telecommunication Union's IMT-2020 standards. Next, let us consider the deployment of 5G, nine companies sell 5G radio hardware and 5G systems for carriers - Altiostar, Cisco Systems, Datang Telecom, Ericsson, Huawei, Nokia, Qualcomm, Samsung and ZTE Large quantities of new radio spectrum (5G NR frequency bands) have been allocated to 5G. 5G devices include Samsung Galaxy S10 5G. The technology is getting adopted and

diffused in Australia, Argentina, Bulgaria, Canada, China, Finland, Germany, India, Monaco, Netherlands, New Zealand, Norway, Pakistan, Philippines, Romania, Russian Federation, San Marino, South Africa, South Korea, Taiwan, Thailand, Uruguay, Vietnam, Qatar, Mexico, USA, Sweden and Panama.

Let us exercise s*cope and usage scenario analysis* of 5G. ITU-R has defined three main uses for 5G as faster and reliable connection - Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). Only eMBB is deployed in 2019; URLLC and mMTC are several years away in most locations. eMBB uses 5G as a progression from 4G with faster connections, higher throughput, and more capacity; mMTC is expected to connect a large number of low power and low cost devices which have high scalability and increased battery lifetime in a wide area. 5G technology may connect some of 50 billion connected IoT devices. The other interesting uses are drones in disaster management through real-time data communication, smart cities for monitoring air and water quality through sensors, Vehicle-to-Vehicle (V2V) communication, public safety (e.g. Mission-critical push-to-talk (MCPTT) and mission-critical video and data), healthcare (Ultra-Reliable Low Latency Communications [URLLC] may improve telehealth, remote patient monitoring, remote surgery and wearable computing applications), fixed wireless connections, smart home (automated home equipped with lighting, heating, or other electronic devices that can be controlled remotely by smartphone or computer).

Most cars are expected to have a 4G or 5G cellular connection for many services. 5G Automotive Association have been promoting the C-V2X communication technology. It provides for communication between vehicles and communication between vehicles and infrastructures, leading to increase in autonomous self-driving cars and IOT (Internet of Things). The speed of 5G technology in upcoming self-driving cars may be vital in helping the capabilities of autonomous cars realize their full potential (Llanasas, 2019). Current 4G network doesn't possess the required speed needed to provide self-driving vehicles that could prevent catastrophic accidents or collision (Llanasas, 2019. 5G is expected to be the basic building block of anti collision system of next generation vehicles.

So far, we have discussed the strength of the emerging wireless technologies. But, there are various constraints such as *interference, security, surveillance* and *health concerns*. The spectrum used by remote sensing, weather and Earth observation satellites will be significant without effective controls. The technology has health concerns; the radiation could have adverse health effects. There are concerns of data security and privacy, surveillance concerns, threats of potential espionage of foreign users by 5G equipment vendors (e.g. Australia, UK and India have taken actions to restrict or eliminate the use of a vendor's equipment in their 5G networks).

***Cloud Computing, Cloud Streaming & Cloud Analytics* : The technologies of cloud computing, cloud streaming and cloud analytics are closely associated. It is an interesting instance of technology association. With the significant advancement of information and communication technology, computing is perceived to be used as the next utility after water, electricity, gas and telecommunication. The concept can**

be extended to cloud computing and grid computing for a market oriented grid. Cloud computing uses the concept of *utility computing*, *fog computing*, *grid computing* and *utility computing* [1-24]. Utility computing is associated with a parallel and distributed system that enables the sharing, selection and aggregation of geographically distributed autonomous computational resources dynamically at runtime depending on their availability, capability, performance, cost and quality through web service. The computational resources include different types of sophisticated software applications such as data mining, scientific computing and image processing, data, CPU or processing power, servers, storage devices, scanners, UPS and network interfaces which can be shared through web service. The objective of utility computing is to provide computing power and storage capacity that can be used and reallocated for any application and billed on a pay-per-use basis. Utility computing consists of a virtualized pool of information systems and other IT resources that can be continually reallocated to meet changing business and service needs of the consumers. These resources can be located anywhere and managed internally or externally. The service provider tracks the usage of computational resources of the consumers and makes invoice based on predefined price setting and usage data. An efficient resource management system coordinates and monitors the complex operation.

Utility computing supports virtualization. Cloud computing is basically a distributed computing where dynamically scalable and virtualized resources are provided as a service over the internet to achieve cost saving, easy scalability and high availability. The services offered through cloud computing usually include Software-as-a-Service (SaaS), Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), data-Storage-as-a-Service (dSaaS) and database-as-a-service (DaaS). SaaS allows users to run applications remotely from the cloud. IaaS provides a set of computing resources as a service which includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access. PaaS includes operating systems and required services for particular applications along with data security, backup and recovery, application hosting and scalable architecture. dSaaS provides data storage, data warehousing and data mining facilities. This is a cost effective, innovative IT infrastructure from which the consumers are able to access desired computational resources and from anywhere in the world on demand.

The key technologies that enable cloud computing are virtualization, web service, service oriented architecture, service flows and work flows. The trading in cloud computing depends on several technological issues such as high availability of service, business continuity, data lock-in, security and privacy of data, efficient data transfer, performance predictability, scalable storage, efficient bugs management in large distributed system, adaptive scaling of operation, innovative software licensing and reputation mechanisms. Strategic pricing considers all these QoS factors to define optimal price setting for cloud computing. In fact, an intelligent, innovative competitive pricing mechanism and highly secure QoS can make cloud computing an attractive IT business model as compared to traditional corporate computing model based on direct IT investment. Nowadays, pay-for-use or pay-as-you-go licensing are becoming popular in cloud computing market. Thus, the

computing world is rapidly transforming towards developing information systems to be consumed as a service. Various service providers have started to build scalable data centers at various locations for hosting cloud computing.

The key players of the market of cloud computing are a set of service providers, service consumers and resource brokers. There are several challenges of trading in cloud computing : fair resource allocation protocols, optimal task scheduling, tendering, contract net protocols, auction, market clearing and negotiation mechanisms and pricing algorithms. The major threats are reduced contract duration, uncertainty, risk and variable duration of a portfolio of contracts, reduced switching costs and customer lock-in, uncertain customer demand, short life-cycle and high sunk cost. Cloud computing may require high development cost for instrumentation, provisioning and monitoring and start up costs in the face of uncertain demand. Cloud computing, web technologies and internet are expected to be extremely useful in higher education, R&D and efficient knowledge management (creation, storage, sharing, transfer and application of knowledge) in terms of innovative multi-dimensional education methodologies (e.g. projects, case discussion, consulting assignments), sources of high quality online education materials, provision of sophisticated softwares for data analysis and data visualization techniques (e.g. Youtube, online test and evaluation).

***Cloud streaming*: Cloud based mobile video streaming techniques are used in online gaming, videoconferencing, augmented reality and watching videos (e.g. movies, music) through smart phones (e.g. mobile visual search smart phones, Tablets). The scope of cloud streaming may be explored through a set of technologies such as mobile multimedia, wireless network, cloud computing, video streaming and video sharing technologies. In mobile communication network, video sharing is done through wireless link (e.g. 3G, 4G, Wi-Fi); on-demand, dynamic and easily accessible video data are provided through streaming protocols in cloud environment. Mobile devices have various constraints such as computation, memory and energy capacity. Mobile cloud computing paradigm is used in transmission of real-time data (e.g. audio, video, text, GPS) transmission; it is bridging the gap between the demand of the service consumers and capability of various mobile devices in terms of data storage and processing of video and audio data.**

***Edge Computing* : Edge computing is a distributed computing paradigm which enables computation and data storage closer to the location where it is needed; improves response times and saves bandwidth. It supports data processing at or near the source of data generation. IoT connected devices interact with remote sensors and may generate data. Edge computing is a perfect fit for IoT - data is processed near the point of origin, the latency between devices and data processing layer is reduced and enable faster response and correctness in decision making. The increase of IoT devices at the edge of the communication network may generate massive amount of data to be computed to data centers and may result the constraints of network bandwidth. Data centers may not guarantee acceptable transfer rates and response times. The devices at the edge constantly consume data**

from the cloud and demand the development of content delivery networks to decentralize data and service provisioning.
The basic objective of edge computing is to move the computation away from data centers towards the edge of the network through a set of smart objects, smart phones and network gateways to perform various tasks such as service delivery, storage and IoT management and ensure improved response time and transfer rate. But there are various news issues in distributed computation such as security and privacy of data, scalability, resiliency, reliability and consistency of system performance. The data should be encrypted for the protection from hacking but it may result increased cost of computation and communication. Scalability in a distributed network should consider different constraints of system performance, energy constraints, dynamic data management and heterogeneity of IoT devices. The system should be protected in terms of liveness, fast fault detection and recovery and stability of the topology of entire distributed system. It is interesting to explore the applications of edge computing in cloud streaming, smart cities and villages and home automation systems.

Internet of Things (IoT), IIoT, RFID, Sensors : Internet of Things (IoT) is a system of interrelated computing devices, mechanical, electrical, electronics and biomedical machines, objects, animals and people with unique identifiers (UIDs) with the ability to transfer data over a network without human-to-human or human-to-computer interaction. IoT has been evolving due to the convergence of multiple technologies such as real-time analytics, machine learning, sensors, embedded systems, wireless sensor networks, control systems, automation (home and building automation), smart home (e.g. lighting fixtures, thermostats, home security systems, cameras), smart phones and smart speakers. But, there are constraints of information security and privacy. The technology has been evolving through R&D on RFID, sensor networks and Industrial IoT (IIoT). The technologies of RFID and sensors are applicable to real-time supply chain management, tracking and inventory management in logistics and retail sectors. Sensor networks can be used for real-time monitoring in defense sector and intelligent military applications. It is also interesting to deploy intelligent sensor networks (e.g. webcams, CCTVs) for real-time surveillance and development of smart cities and smart villages and intelligent transportation networks.

Information technology

Analytics: **Analytics is one of the most promising digital technologies today. The technology is going through an evolution of various phases such as shallow, predictive, collaborative, big and deep analytics. Deep analytics is an intelligent, complex, hybrid, multi-phased and multi-dimensional data analysis system. The basic steps of computation are data sourcing, data filtering / preprocessing, data ensembling, data analysis and knowledge discovery from data. The authorized data analysts select an optimal set of input variables, features and dimensions (e.g. scope, system, structure, security, strategy, staff-resources, skill-style-support) correctly being free from malicious attacks (e.g. false data injection, shilling); input data is**

sourced through authenticated channels accordingly. The sourced data is filtered, preprocessed (e.g. bagging, boosting, cross validation) and ensembled. It is rational to adopt an optimal mix of quantitative (e.g. regression, prediction, sequence, association, classification and clustering algorithms) and qualitative (e.g. case based reasoning, perception, process mapping, SWOT, CSF and value chain analysis) methods for multi-dimensional analysis. The analysts define intelligent training and testing strategies in terms of selection of correct soft computing tools, network architecture – no. of layers, nodes; training algorithm, learning rate, no. of training rounds and stopping criteria;. The hidden knowledge is discovered from data in terms of collective, collaborative, machine, security and business intelligence. The analysts audit fairness and correctness of computation and also reliability, consistency, rationality, transparency and accountability of the analytics.

Deep analysis (e.g. in memory analytics) can process precisely targeted, complex and fast queries on large (e.g. petabytes and exabytes) data sets of real-time and near real-time systems. For example, deep learning is an advanced machine learning technique where artificial neural networks (e.g. CNN) can learn effectively from large amount of data like human brain learn from experience by performing a task repeatedly and gradually improves the outcome of learning. Deep analytics follows a systematic, streamlined and structured process that can extract, organize and analyze large amount of data in a form being acceptable, useful and beneficial for an entity (e.g. individual human agent, organization or BI information system). It is basically a specific type of distributed computing across a number of server or nodes to speed up the analysis process. Generally, shallow analysis use the concept of mean, standard deviation, variance, probability, proportion, pie chart, bar chart and tables to analyze small data set. Deep analytics can analyze large data sets based on the concepts of data visualization, descriptive and prescriptive statistics, predictive modeling, machine learning, multilevel modeling, data reduction, multivariate analysis, regression analysis, logistic regression analysis, text analysis and data wrangling. Deep analytics is often coupled with business intelligence applications which perform query based search on large data, analyze, extract information from data set hosted on a complex and distributed architecture and convert that information into specialized data visualization outcome such as reports, charts and graphs.

Collaborative analytics is a set of analytic processes where the data analysts work jointly and cooperatively to achieve shared goals through data sharing as per revelation principle, privacy and information disclosure policy, collective analysis and coordinated decisions and actions. Collaborative analytics allows sharing of strategic information among various phases of data analysis such as demand planning of data, data sourcing, organizing data, exception management, data warehousing, execution of data analysis, reporting conclusions and determining actions. The data loop promotes data sharing to avoid redundancy. Communication and sharing improves reliability and consistency of data analysis across an organization. The analysis loop explores insights in terms of multi-dimensional analysis through a recursive process of developing and validating hypotheses for robust and complete conclusions. The action loop focuses on coordination of complete and connected set of actions across an organization through better

understanding and in-depth analytical skills. Conventional analytics explore hidden intelligence of data to make rational decisions. Collaborative analytics is focused on increased coordination, cooperation and integration among various units to improve alignment of decisions and actions across entire business unit.

Information Security Intelligence (ISI) Analytics: **ISI analytics is an emerging digital technology; its scope may be analyzed in terms of adaptive security, dynamic data protection, self-healing mechanism and crash proof codes. An enterprise information system may face various threats of malicious attacks from external and internal environments; it is essential to protect the system through ISI analytics. ISI analytics monitors enterprise information system in real-time to detect any anomalies and vulnerabilities. If a threat is detected, ISI analytics should be able to mitigate the risks through a set of measures. Let us consider the technology of crash proof codes which verify the reliability of an operating system through formal verification methods. The concept is applicable to the operating system designed for processors embedded in smart phones, vehicles, aircrafts, drones and medical devices where software bugs can be disastrous and unnecessarily risky programs may put lives in danger. Is it possible to mitigate the risks by making kernel i.e. the core component of an operating system in such a way that it will never crash? Section 4 outlines the concept of adaptive analytics and dynamic data protection. Session 3 highlights self-healing mechanism of a smart grid.**

Applied AI, Deep learning & Robotics : **AI simulates human intelligence and develops algorithms that learn and perform intelligent behavior with minimal human intervention, high precision, accuracy and speed. Robotics is an interdisciplinary branch of mechanical, electrical and electronics engineering and computer science. The basic objectives of Robotics are design, construction, operation and use of robots and related information system for control, sensory feedback, and information processing; human robot interface, mobility, manipulation, programming and sensors development. Various domains of artificial intelligence (AI) are being used in Robotics such as computer vision, NLP, Edge computing, deep, transfer and reinforcement machine learning. A robot is a programmed machine designed to execute one or more tasks automatically and repeatedly with speed and precision. There are as many different types of robots. Engelberger and George Devol developed first industrial robot; there are different types of industrial robots such as cartesian, SCARA, cylindrical, delta, polar and vertically articulated. The basic components of a robot are controller (or brain run by a computer program); robotic operating system; electrical parts such as motors, sensors for sensing and touch, power sources (e.g. solar cells, pneumatics, flywheel, hydraulic); mechanical parts such as actuators, effectors, grippers, manipulators, air muscles, muscle wire, pistons, grippers, wheels, and gears that make the robot move, grab, turn and lift and locomotion : walking, hopping, dynamic balancing, flying, snaking, skating, climbing, swimming and sailing. Robotics is extensively used in automotive industry in various types of applications such as collaborative robots, painting, welding, assembly, material removal, parts transfer and machine tending. Medical robots are used for delicate surgical operation in healthcare.**

Robots can substitute for humans and replicate human actions in dangerous environments (e.g. bomb detection and deactivation, toxic manufacturing environment or where humans cannot survive such as space, under water, high heat, hazardous materials and radiation) and other various types of interesting application (e.g. Cobots, Nano robots, autonomous drones in defense and bio-inspired robots). The advantages of robotics include the execution of heavy duty jobs with precision, repeatability, reliability and consistency. Is it possible to develop robots with intelligent human skills such as innovation, creativity, decision making, flexibility and adaptability, speech and voice recognition, gestures, facial expression, artificial emotions, personality and social intelligence? This is an interesting open agenfa for future generation robotics technology.

Miscellaneous

***Solar Computing*: Solar computing is an emerging technology which should be able to interact with the consumers of energy on various issues such as demand response schemes, current energy sources, information on availability of power, peak load, energy consumption, payments, discounts, variable pricing mechanisms and charging of electrical and hybrid vehicles. The objective of demand response schemes is to accommodate variable supply of renewable energy sources and high frequency monitoring of demand and supply for smart homes, buildings and micro-grids. Solar computing is associated with various types of emerging applications such as internet of energy, smart homes and autonomous micro-grids to manage and monitor the use, storage and production of electrical energy though a network of automated modules. It is essential to explore the scope of solar computing from different perspectives such as sustainability, efficiency, stability, reliability and consistency of generation, transmission, distribution and consumption of power in a complex and dynamic business environment; threats of climate change; challenges of integration between conventional energy grid and renewable energy sources, energy policy and market mechanisms. The scope of solar computing spans over several factors such as demand and supply management, electrical and hybrid vehicles, virtual power plants, prosumers and self healing networks, increased demand of electrical energy, extensive use of intermitted, distributed, clean and time variable renewable energy. The ultimate objective is to match demand with supply. A smart grid may consist of thousands of generators, power transmission and distribution network and distributed network of prosumers. The other important objectives of solar computing are to build a clean and efficient power grid for smart life-style that can support bi-directional flow of both electrical energy and information for real-time demand and supply management at economies of scale through intermittent renewable sources. Solar power is an interesting option for running computers in rural area and remote zone (e.g. forest, hills, desert, sea coast). Is it possible to explore a highly energy efficient, low cost (e.g. operation, transport and service), lightweight, rugged and reliable system that can run from direct current generated by solar panels and smart batteries in a hot and dusty hazardous environment?**

***Virtual and augmented reality*: VR and AR are sophisticated, creative and powerful tools to offer digital experience by integrating AI, computer vision, graphics and automation in various applications such as manufacturing, retail, healthcare and entertainment. These reality technologies can effectively support direct-to-consumer e-commerce models through vertical integration bypassing tiers of supply chain at reduced costs and enhanced profit margin. Virtual reality technology provides immersive and interactive experiences to the human agents through computer graphics or visual elements and support V-Commerce business models through an alternate technology platform. Voice activated commerce (e.g. voice logistics for warehouse management system) uses natural language processing, speech and voice recognition technologies for the interaction between the users and commercial platforms and applications. It is an interesting agenda to broadcast the programmes of religious and cultural festivals, carnivals and special events to the viewers using the concept of virtual reality to avoid the hassles in crowd control.**

***Digital twins*: How is it possible to represent the structure of a system associated with a technology innovation correctly and transparently? Digital twins may be an interesting solution; it integrates the concept of industrial IoT, AI, machine learning and software analytics to optimize the operation and maintenance of physical assets, systems and manufacturing processes. A digital twin is the digital replica of a living or non-living physical entity (e.g. physical asset, process, agent, place, system, device); it is expected to bridge and support data sharing between the physical and virtual entities. Digital twins can learn from multiple sources such as itself through sensors, historical time series data, experts and other nodes of the networking schema of the system and get updated continuously to represent real-time status, working conditions or positions.**

The concept of digital twins are expected to be useful for manufacturing, energy (e.g. HVAC control systems), utilities, healthcare and automotive industries in terms of connectivity, digital traces and product life-cycle management. The concept can be used for 3D modeling to create digital companions of the physical objects i.e. an up-to-date and accurate copy of the properties and states of the objects (e.g. shape, position, gesture, status, motion) based on the data collected by the sensors attached to the system. It may be useful for the maintenance of power generation equipment such as turbines, jet engines and locomotives; monitoring, diagnostics and prognostics to optimize asset performance and utilization through root cause analysis and to overcome the challenges in system development, testing, verification and validation for automotive applications. The physical objects are virtualized and can be represented as digital twin models seamlessly and closely integrated in both physical and cyber spaces. Digital twins should represent the structure of a product innovation intelligently through various phases of the product life-cycle.

***Ray tracing* : In computer graphics, ray tracing is a rendering technique to generate an image by tracing the path of light as pixels in an image plane and simulate the effects with virtual objects. The technique can create a very high degree of visual effects at high cost of computation. This concept is useful for film, TV and video games applications. Ray tracing can simulate various optical effects like reflection, refraction, scattering, and dispersion.**

***Quantum computing*: Quantum computing is a promising technology to solve computation problems significantly faster as compared to classical computers. This technology is based on the concepts of quantum mechanical phenomena such as superposition and entanglement to process data efficiently. Quantum theory analyzes the nature of energy and matter on the atomic and subatomic level. Quantum computing is a branch of quantum information science (e.g. quantum cryptography, quantum communication). In a classical computer, Boolean logic is represented through a set of bits where each bit is either 1 or 0. Quantum computers are not limited to two states and encode information as quantum bits. Qubits are the basic building blocks of quantum computing. Qubits can be in a 1 or 0 quantum state; can also be in a superposition of 1 and 0 states. When qubits are measured, the result is always either 0 or 1; the probabilities of the two outcomes depend on the quantum state of the qubits. Qubits represent atoms, ions, photons or electrons that work together to act as computer memory and a processor.**

***Solar computing - self-healing mechanism for a smart grid* : Please refer to session 6 which evaluates the potential of solar power technology in terms of solar power electronics and nanotechnology of solar cells. This session explores the technology of solar computing; which is basically the support of digital technology for solar power system. Solar computing is an emerging technology which should be able to interact with the service consumers on various issues such as solar and grid energy sources, demand response schemes, information on availability of power, peak load, energy consumption, payments, discounts, variable pricing mechanisms and charging of electrical and hybrid vehicles. The objective of demand response schemes is to accommodate variable supply of renewable energy sources and high frequency monitoring of demand and supply for smart homes, buildings and micro-grids. Solar computing is associated with various types of emerging applications such as internet of energy, smart homes and autonomous microgrids to manage and monitor the use, storage and production of electrical energy though a network of automated modules. It is essential to explore the scope of solar computing from different perspectives such as sustainability, efficiency, stability, reliability and consistency of generation, transmission, distribution and consumption of power in a complex and dynamic business environment; threats of climate change; challenges of integration between conventional energy grid and renewable energy sources, energy policy and market mechanisms. The scope of solar computing spans over several factors such as demand and supply management, electrical and hybrid vehicles, virtual power plants, prosumers and self healing networks, increased demand of electrical energy, extensive use of intermitted, distributed, clean and time variable renewable energy. The ultimate objective is to match demand with supply. A smart grid may consist of thousands of generators, power transmission and distribution network and distributed network of prosumers. The other important objectives of solar computing are to build a clean and efficient power grid for smart life-style that can support bi-directional flow of both electrical energy and information for real-time demand and supply management at economies of scale through intermittent renewable sources. Solar power is an interesting option for running computers in rural area and remote zone (e.g. forest, hills, desert, sea coast)**

and maximum power point tracking (MPPT) is a critical function of solar computing. Is it possible to explore a highly energy efficient, low cost (e.g. operation, transport and service), lightweight, rugged and reliable system that can run from direct current generated by solar panels and smart batteries in a hot and dusty hazardous environment?

This session shows the application of deep analytics [7-S], SWOT analysis and technology life-cycle analysis on the technological innovation of a self-healing smart power grid from the perspective of solar computing. We have done the scope analysis of the technological innovation on a smart power grid in terms of self-healing mechanism, solar computing, demand supply management, virtual power plants, electrical and hybrid vehicles and energy prosumers. This work also shows the analysis on adaptive security and dynamic data protection, strategy, staff-resources and skill-style-support for the innovation, adoption and diffusion of solar computing. It is essential to verify the security intelligence of the power grid at multiple levels and assess the risks of various types of threats from the perspectives of over current, earth fault, short-circuit, voltage, reactive power and distance protection. Finally, this work outlines a self-healing mechanism [SHM] based on case study and review of relevant works on security of smart grid. The key focus areas are solar computing, smart solar grid, self-healing mechanism, adaptive security, dynamic data protection, maximum power point tracking, AI, threat analytics, digital relay protection and Green IS.

What is a smart grid in the context of solar computing? What is the problem of technology innovation of solar computing and a smart power grid? A smart grid is a fully automated power delivery network that monitors and controls a set of nodes, supports a bidirectional flow of electricity and information between the power plants, loads and all intermittent points. Today's smart grid needs the support of distributed intelligence, broadband communication and automated control system for real -time market transactions and seamless interfaces among people, building, industrial plants, power generation, transmission and distribution networks. There are various types of challenges, complexities, constraints, security and privacy issues in power system engineering, telecommunication, cyber security, distributed intelligence, automation and information exchange among various system components of a smart grid.

It is essential to explore the scope of a smart power grid from different perspectives such as sustainability, efficiency, stability, reliability and consistency of generation, transmission, distribution and consumption of power in a complex and dynamic business environment; strength, weakness, opportunities, threats of climate change, natural disasters and acts of terrorism; challenges of integration between conventional energy grid and renewable energy sources, energy policy and market mechanisms (e.g. dynamic pricing, swing option, trading agent competition); emerging applications such as electrical and hybrid vehicles; supply chain planning, collaboration, execution and resource management; various scopes of energy informatics and green information system; computing methodologies (e.g. AI, machine learning), data, networking and security schema, application integration and intelligent analytics.

Typically, the scope of a smart grid spans over several factors such as demand and supply management, electrical vehicles, virtual power plants (VPP), prosumers and self healing networks, increased demand of electrical energy, extensive use of intermitted, distributed, clean and time variable renewable energy. The ultimate objective is to match demand with supply. A VPP may consist of thousands of generators, power transmission and distribution network and distributed network of prosumers (both consume and produce power). The other important objectives are to build a clean and efficient power grid for smart life-style that can support bi-directional flow of both electrical energy and information for real-time demand and supply management at economies of scale through intermittent renewable sources. It is essential to develop a set of coordination mechanisms for a decentralized, autonomous and intelligent smart power grid.

Let us explore the scope of Artificial intelligence (AI) for a smart power grid. AI is basically the simulation of human intelligence. It represents and executes a processes through machines. The objective of AI is how to make computers do things at which, at the moment, the people are better. A smart grid system is expected to be an intelligent knowledge based system having a set of features from the perspectives of AI: ability of learning and understanding from experience, rational reasoning, making sense out of fuzzy data or approximate reasoning, adaptive system performance i.e. sense and respond, analytical, logical and case base reasoning in solving problems and ability in dealing with complex situations. Is it possible to develop a smart grid that can mimic human intelligence? Another critical issue is heuristics search; heuristics are intuitive knowledge or rules of thumbs learnt from experience; it can reduce the complexity of problem solving. It is not required to rethink completely to solve a problem of a smart grid if it occurs repeatedly.

Adaptive security for IIoT enabled SCADA & industrial control system : **Information Security Intelligence (ISI) analytics is an emerging digital technology; its scope is analyzed in terms of adaptive security and dynamic data protection. Supervisory Control & Data Acquisition (SCADA) & Industrial Control System (ICS) may face various threats of malicious attacks from external and internal environments; it is essential to protect the system through ISI analytics. ISI analytics can monitor SCADA / ICS in real-time to detect any anomalies and vulnerabilities. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities. This session is focused on digital defense of Industrial Internet of Things (IIoT) enabled SCADA and Industrial Control System (ICS), an emerging technology in energy, utility, defense, transportation and financial service sectors. The complexity of this technology has been analyzed through deep analytics along seven 'S' dimensions: scope, system, structure, strategy, security, staff-resources and skill-style-support. It highlights technology life-cycle analysis on S-Curve; the technology is passing through growth phase at present. The complexity of technology has been analyzed based on related literature review on IIoT, SCADA and ICS and also reasoning of three cases: (a) SCADA for a smart power grid, (b) adaptive industrial control system (ICS) and (c) border security surveillance in defense. We have also outlined**

security intelligence verification mechanism (SIVM) of IIoT enabled SCADA and ICS based on an adversary model and intelligent threat analytics. The key focus areas are ISI analytics, adaptive security, dynamic data protection, industrial Internet of Things, SCADA, industrial control system, deep analytics, threat analytics, adversary model, security intelligence verification algorithm, defense, smart power grid, fuzzy control and expert System.

The basic objective of the technological innovation of ISI analytics is to verify the security intelligence of SCADA and industrial control system so that the assets of information and communication technology of an enterprise are protected from various types of malicious attacks. ICS & SCADA performs key functions to provide essential services such as defense, energy (e.g. smart power grid), utilities, transportation and communication system of a country. It is a part of a nation's critical infrastructure and operates with the support of industrial control systems, supervisory control and data acquisition (SCADA), sensor networks, information and communication technologies. ICS / SCADA systems are potentially vulnerable to various types of malicious attacks which may affect the safety of common people and the performance of critical infrastructure seriously and may cause huge financial loss.

Any comprehensive and complete solutions are missing in the existing works for the verification of security intelligence of SCADA / ICS. The present work evaluates the technology associated with IIoT enabled SCADA / ICS and also outlines algorithmic security intelligence verification mechanism (SIVM) in terms of system, input, output, objectives, constraints, moves, revelation principle, payment function, security intelligence and proactive and reactive risk mitigation approaches. The security intelligence of ICS / SCADA is explored in association with computing, data, networking, application and security schema at five levels : L1, L2, L3, L4 and L5 in terms of intrusion and access control, secure multi-party computation, system performance, malicious attacks and multi-party corruption respectively through an intelligent threat analytics. The present work assesses the risk of different types of threats on ICS / SCADA and presents a set of intelligent verification mechanisms which can protect the system from potential malicious attacks. The verification mechanisms are based on cryptography and distributed secure multi-party computation. An efficient system is expected to be resilient. Resiliency measures the ability to and the speed at which the system can return to normal performance level following a disruption. The vulnerability of the system to a disruptive event can be viewed as a combination of likelihood of a disruption and its potential severity.

Let us first present a deep analytics for IIoT enabled ICS and SCADA. It is basically an integrated framework which is a perfect combination or fit of seven factors. A complex operation of ICS and SCADA may fail due to the inability of the system administrator to recognize the importance of the fit and the tendency to concentrate only on a few of these factors and ignore the others. These factors must be integrated, coordinated and synchronized for effective SCADA operation. The panel has defined the technology of IIoT enabled SCADA and ICS. They have analyzed the technology through scope, system, structure, strategy, security, staff-resources and skill-style-support respectively. Section 5 outlines security intelligence verification mechanism (SIVM). They have also analyzed three test cases: (a)

SCADA for a smart power grid, (b) industrial control system and (c) defense for border security surveillance.

Supervisory control and data acquisition (SCADA) networks perform key functions to provide essential services for energy and utilities (e.g. electricity, oil, gas, water), defense and communication sectors. SCADA is a part of a nation's critical infrastructure and operates with the support of industrial control systems, sensor networks and information and communication technologies. SCADA networks are potentially vulnerable to various types of malicious attacks that result disruption of critical security services in terms of confidentiality, integrity, availability, authentication, non-repudiation, access and inference control, intrusion, process redirection or manipulation of operational data. These attacks may affect the safety of common people and the performance of critical infrastructure seriously and may cause huge financial loss. Therefore, the protection of SCADA networks should be a national priority.

Industrial control systems for critical infrastructure like national power grid make increasingly use open technologies and Internet protocols. A smart energy grid often faces the challenge of malicious attacks (e.g. cyber attack) from power play and politics, industrial espionage and terrorists and also compromises of information infrastructure due to user errors, equipment failure and natural disaster. A malicious agent may be able to penetrate an energy grid, gain access to control software and hardware and alter load conditions to destabilize the grid in an unpredicted way.

Let us analyze the scope of IIoT technology. Internet of Things (IoT) is a networked smart devices equipped with sensors and RFID tags, connected to the Internet, all sharing information with each other without human intervention, dynamic global network infrastructure with self configuring capabilities, standard interoperable communication protocols, intelligent interfaces and are seamlessly integrated with information network. The fast development of networked smart devices with Internet, sensors and radio frequency identification devices (RFID) is enabling the emergence of many new applications in remote access control, effective monitoring and supervision, better performance, real-time decision making, system integration and access to cloud based resources. IIoT is used for various types of industrial applications such as aerospace and aviation, airports, automotive, environment monitoring, food technology, smart cities, intelligent buildings, intelligent transportation infrastructures, healthcare, operation in hazardous environment, retail, logistics, supply chain management and monitoring of safety and security of plant (e.g. advanced metering, energy management, interaction with smart appliances).

Next, let us explain the scope of digital defense: how to protect information and communication technology (ICT) assets of an enterprise from various types of malicious attacks. Why should a business model address information security in an effective and comprehensive way? It is basically a problem of risk management; attacks on ICT technology schema and the theft or misuse of critical data should be assessed and mitigated appropriately for digital transformation. Digital defense is associated with a complex process which includes identification of information assets, assessment of critical vulnerabilities, selection of appropriate security

solution for the protection of ICT schema, trusted computing environment development, preserving the authenticity, authorization, correct identification, privacy and audit of electronic transactions, access control and defining security policy, process and maintenance intelligently [1]. This work talks about traditional issues of user permission control, confidentiality by encryption, authorization through passwords, tokens, digital certificates, role based access control, audit trails and digital signature for the protection of general information assets such as data on sales, customers, vendors and human resources.

The existing works have been reviewed on system architecture, computational intelligence of verification mechanisms, potential threats and vulnerabilities, security concerns and risk analysis of various types of industrial control systems and SCADA. The review of existing literature could not find out an efficient mechanism for SCADA / ICS. The existing works have several gaps. The security intelligence is expected to be defined strongly with robustness, completely and precisely. The protocols should have intelligent model checking or system verification strategies based on rational threat analytics. The present work has identified three critical issues to be associated with digital defense of information and communication technology assets of ICS and SCADA: threats analytics, verification mechanisms of security intelligence and relevant computational challenges. Case based reasoning approach is adopted also for experimenting three test cases on smart power grid, industrial plant and defense SCADA.

This session assesses the risk of different types of threats on ICS & SCADA and presents a set of intelligent verification mechanisms which can protect the system from potential malicious attacks. The mechanisms are based on cryptography and distributed secure multi-party computation and check the security intelligence of a resilient system from the perspectives of intrusion detection, secure communication, service oriented computing, credential based biometric access control, privacy and inference control. The research methodology adopted in the present work includes case analysis and review of relevant literature. The logic of the verification mechanisms has been explored through analysis of three cases.

Secure Multi-party Quantum Computing for authentication through signcryption: **This session analyzes the complexity and potential of secure multi-party quantum computing (SMQC) technology in terms of seven elements of deep analytics : scope, system, structure, security, staff-resources and skill-style-support. Quantum computing is a promising technology to solve computation problems significantly faster as compared to classical computers. The technology is at emergence phase of S-curve. This session explores a set of interesting scope of secure multi-party quantum computing : how to construct various concepts of cryptography such as encryption and decryption, digital signature, signcryption, authentication, zero knowledge proof and oblivious transfer in the context of secure multi-party quantum computing? How to construct secure multi-party quantum computing protocols verifying security intelligence at various levels : L1 (access control), L2 (computational intelligence), L3(system performance), L4(malicious attacks) and L5(multi-party corruption)? This session presents SMQC algorithm and analyzes the complexity of the algorithm in terms of verification of security intelligence. The**

key focus areas are secure multi-party computing, quantum computing, information theory, secret sharing, authentication, signcryption, authorization, correct identification, privacy, audit and multi-party corruption.

Secure multiparty computation allows a group of mutually distrustful parties to perform correct, distributed computations under the sole assumption that some parties will follow the protocol honestly. It has been studied extensively in the classical setting and may be extended to the setting of quantum computing. A secure quantum multiparty protocol allows n parties $P_1, \ldots, P_n$ to compute an n input quantum circuit where each party P_i is responsible to provide one of the input states. The output of the circuit is decomposed into n components $H_1 \otimes \ldots \otimes H_n$ and P_i receives the output H_i. There exists pairwise quantum channels and a classical broadcast channel among n parties, there exists a universally composable, statistically secure multiparty quantum computation protocol that tolerates an adaptive adversary controlling up to $t < n / 2$ faulty parties.

The complexity of the protocol is polynomial in terms of the number of parties and the size of the circuit. The critical issue is how much trust is necessary for secret sharing : how many parties must remain honest for distributed quantum computation. A verifiable quantum secret sharing protocol and a general secure multiparty quantum computing protocol can tolerate any $\lfloor (n-1)/2 \rfloor$ cheaters among n parties Is it possible to improve the threshold of an efficient secure multiparty quantum computing protocol? The scope of secure multi-party quantum computing may be explored in terms of a set of open issues : how to construct various cryptographic algorithms such as encryption and decryption, digital signature, signcryption, authentication, authorization, correct identification, privacy, secret sharing, zero knowledge proof and oblivious transfer in the context of secure multi-party quantum computing? How to tailor secure multi-party quantum computing protocols verifying security intelligence at various levels : L1 (access control), L2 (computational intelligence : fairness, correctness, transparency, accountability, rationality, trust), L3(system performance : reliability, consistency, resiliency). L4(malicious attacks : Sybil attack, false data injection attack, denial of service attack) and L5(multi-party corruption)? How to construct the protocols of oblivious transfer, secure function evaluation, mixnet and private comparison protocols in the setting of secure multi-party quantum computing? The next section presents Secure Multi-party Quantum Computing (SMQC) algorithm where a client sendS challenge to an administrator of private data schema and receives authenticated response. Authentication is done through signcryption algorithm.

***Secure adaptive filter in adversarial environment – threat analytics*: This session analyzes the complexity and potential of secure adaptive filter in adversarial environment in terms seven elements of deep analytics : scope, system, structure, security, staff-resources and skill-style-support. The contributions of this work is follows. The scope of adaptive filters has been analyzed in terms of a set of interesting data base and communication networking applications, distributed systems, data streaming, packet classification, spam filtering and web caching. The system element presents algorithmic secure adaptive filter mechanism which**

outlines two differe types of filter : (a) private search and (b) optimal margin classifier enabled private search. We have explored whether private Support Vector machine based on optimal marging classifier can be applied to the problem of packet classification in communication networks. The structure element highlights various types of filters such as Bloom, Cuckoo, Adaptive Cuckoo and parallel D-piepline and their strength and weakness. The technology is at emergence phase of S-curve. This work also outlines how to verify the security intelligence of adaptive filter at multiple levels : L1 (access control), L2 (computational intelligence), L3 (system performance), L4 (malicious attacks) and L5(multi-party corruption). Specific focus has been given to correctness (e.g. false positive and false negative) and privacy of computation by the adaptive filter. The correctness of the filter is deeply associated with right configuration of the data schema. The privacy of computation can be ensured through a robust revelation principle of the filter. The key focus areas are adaptive filter, bloom filter, cuckoo filter, adversarial environment, secure multiparty computation, threat analytics, optimal margin classifer, private support vector machine.

Scope Analytics
Objects **: Secure adaptive filter;**
Scope **: Data base applications, Distributed systems, Data streaming, Communication networking applications, Packet classification, Spam filtering, Web caching**

Secure adaptive filter is a simple space efficient randomized data structure for representing a set to support membership queries. It allows false positives but the saving in space complexity often outweigh this drawback when the probability of an error is made sufficiently low. The scope of secure adaptive filters has been explored in terms of a set of interesting data base and communication networking applications, distributed systems, data streaming, packet classification, spam filtering and web caching. The filters are used for collaborating in overlay and peer-to-peer networks, resource routing, packet routing and measurerement for making data summary in routers and other various types of devices in intelligent communication network. The filters are used as a data structure for approximate set membership by reacting to false positives. The filter is used as data dictionaries in table look up and UNIX spell checkers, as a means of storing a dictionary of unsuitable passwords for information security and also distributed database applications. The filters are also used for distributed web cache sharing protocols, desktop web browsing for P2P/Overlay networks, approximate set reconciliation for content delivery, set intersection for keyword searches, resource routing in P2P networks, geographic routing for mobile computers and packet routing applications (e.g. early detection of forwarding loops in unicast and multicast protocols, queue management, multicast) and to provide a reasonable measuremrnt infrastructure (e,g, recording heavy flows, IP traceback, how many packets from a given flow pass through a router? has a packet from this source passed through this router recently?)

2. SYSTEM

System Analytics

Prof. Simon Watson and Dr.Henry Plank are exploring the systems associated with emerging digital technologies. The basic objectives of digital technology is intelligent decision making in complex and rapidly changing business environment, fast decision making in adaptive situation, improved accuracy in decision making, discovery of hidden intelligence from large pool of data, fast and correct transaction processing; support creation, storage, transfer and application of knowledge in an enterprise, support office automation and efficient management of resources (e.g. man, machine, materials, method and money) of an enterprise. An information system associated with digital technology can be classified into different categories such as transaction processing, decision support, group decision support, knowledge management, knowledge based office automation and business intelligence system. It is possible to analyze digital technology in terms of computing (e.g. centralized, distributed, local, global), data, networking (e.g. wired, wireless, Internet), application (e.g. features, modules, functions, application integration) and security schema.

dSaaS / DaaS **: The basic objective of DaaS is to avoid the complexity and cost of running a database with improved availability, performance, price and flexibility. It gives the access to various types business intelligence solutions (through web) which include distributed database, data warehousing, data mining, business and web analytics, data visualization and business performance measurement applications. The pricing of dSaaS is based on the cost of hardware (e.g. data warehouse, servers), the cost of software (e.g. business intelligence solutions) and system administration cost (e.g. data centre administration, data base security, backup, recovery and maintenance). A consumer can lease a data storage space where it is required to measure different system parameters such as stored data (GB/month) and number of processed queries (per 10k requests / month) to compute the price of dSaaS / DaaS. The provider can offer quantity discount in case of group buying of storage space. The prices of DaaS / dSaaS are also determined by various QoS parameters such as connection speed, data store delete time, data store read time, deployment latency (i.e. the amount of latency between when an application is posted and ready to use) and lag time (how slow the system is). The pricing of dSaaS is also governed by the security and privacy of data. Some applications (e.g. education sector) require low level of privacy of data. Some applications (e.g. financial service, healthcare) need high level of security and privacy in data outsourcing and this involves high cost of computation and communication from the perspectives of statistical disclosure control, private data analysis, privacy preserving data mining, intelligent access control and query processing on encrypted data. The service provider should define a discriminatory pricing mechanism for dSaaS: high level of security and privacy of data demands high price and low level of security asks low price.**

The price of dSaaS is a function of miscellaneous cost elements of a data center. A *data centre* or data bank is the collection of servers where the applications and data are stored. Data center consists of a set of servers and network architecture. The servers store the data from different organizations and network architecture facilitates the services to use, store, and update the data of the servers. The cost of administration of data centre includes several factors: initial development cost, operating cost, maintenance cost and cost associated with disaster recovery plan. The development cost includes the cost that requires making master plan, building infrastructure, buying hardware and software, making database and security schema. Operating cost includes the cost of energy, cooling system, system administrators, software license and network cost. Maintenance cost is the cost of maintaining the system which includes upgradation of hardware and software. One of the most challenging issues of data center management is the resource allocation strategy: how it is possible to cater the demand of the service consumers using minimum number of servers. It has an impact on the size, complexity and cost of data center. The data centre administrator can follow dedicated or shared server allocation strategy.

The price of dSaaS is also a function of energy consumption of cloud computing system in a data center. There are many open challenges of energy efficient design of computing systems and green IT covering the hardware, operating system, virtualization and data center levels. The basic objective of the cloud computing system design has been shifted to power and energy efficiency to improve the profit of the service provider. Energy consumption is not only determined by hardware efficiency, but it is also dependent on the resource management system deployed on the infrastructure and the efficiency of applications running in the system. Solar power electronics is an interesting option of green IT. Higher power consumption results not only high energy cost but also increases the cost of cooling system and power delivery infrastructure including UPS and power distribution panels. The consolidation of IT infrastructure should be done intelligently to reduce both energy consumption and performance degradation through improved power management. Energy consumption can be reduced by increasing the resource utilization and use of energy efficient cloud computing system.

***Software-as-a-Service (SaaS)*: SaaS is an application hosted on a remote server and accessed through web; it can be business service or customer oriented service. The basic objective is to reduce software licensing cost and improve productivity by using sophisticated applications. The pricing strategy of SaaS is based on pay-as-you-go basis; not dependent on number of licensing period and licensing users as in case of direct software procurement. Another concept is *software plus service* where an enterprise uses a locally hosted software application and additionally uses SaaS through cloud for a specific type of application. Using the existing software paradigm, the consumer purchases a software package and license by paying a one-time fee. The software then becomes the property of the consumer. Support and updates are provided by the vendor under the terms of the license agreement. This can be costly if the user is installing a new application on hundreds or thousands of computers. SaaS, on the other hand, has no licensing. Rather than buying the**

application, the consumer pay for it through the use of a subscription based on number of concurrent users and only pay for what is used.

The computation of subscription fee can be *stochastic* pricing or simple *cost* based pricing. The price of SaaS depends on specific business model of the service provider. Suppose, a service provider develops in-house software products. Another service provider buys COTS from third-party vendor based on number of licensed users and licensing period and provides SaaS to the consumers. There may be restriction of number of concurrent users and different subscription rate of SaaS in second case.

This pricing strategy should also consider cost of upgrading software application; the provider may offer incentive for upgrading applications. In case of security software pricing, there may be different alternative strategies to manage network security: (i) consumer self-patching where no external incentives are provided for patching or purchasing, (ii) mandatory patching, (ii) patching rebate and (iv) usage tax. For proprietary software, when the software security risk and the patching costs are high, a patching rebate dominates the other strategies. When the patching cost or the security risk is low, self-patching is the best option.

Stochastic risk based pricing mechanism considers several risk factors and optimizes the expected net present value of revenue subject to maximum acceptable risk of the provider. In this case, the service provider does not give much focus on cost accounting model or profit margin but tests the price sensitivity of the customers experimentally or through trial and error method. The provider does not have any precise perception about the demand of the new software products. But, it follows dynamic risk based pricing based on assessed risks and competitive intelligence. For in-house software development, software cost is a function of efforts on feasibility study, requirement analysis, system design, program design, coding, testing and modification following waterfall / v-process / spiral / proto-typing / incremental delivery model. The service provider estimates effort for a specific SDLC model and then selects an optimal profit margin.

***Infrastructure-as-a-Service (IaaS)*: A cloud computing infrastructure consists of different types of elements: clients (e.g. mobile, PDA, laptop, thin and thick), the data center and distributed servers. *Thin clients* are less costly than thick clients. A growing trend in the cloud computing is *virtualization* of servers. In a virtualized environment, applications run on a server and are displayed on the client. The server can be local or on the other side of the cloud. Software can be installed allowing multiple instances of virtual servers which run on a physical server. Full *virtualization* is a technique in which a complete installation of one machine is run on another. It allows the running of different and unique operating systems. *Hardware-as-a-Service (HaaS)* simply offers the hardware required by a consumer. Cloud computing is a business model of delivering IT resources and applications as services accessible remotely over the Internet rather than locally. IaaS supports remote access of computer infrastructure as a service.**

Cloud computing supports elastically scaling computation to match time varying demand. But, the uncertainty of variable loads necessitate the use of margins i.e. the servers that must be kept active to absorb unpredictable potential load surges which

can be a significant fraction of overall cost. There are challenges of minimizing margin costs and true costs for IaaS. The provider should not adopt a fixed margin strategy; the margin should be load dependent. The margin required at low loads may be higher than the margin required at high loads. Secondly, the tolerance i.e. the fraction of time when the response time target may be violated need not be uniform across all load levels. It is really challenging to achieve optimal margin cost while guarantying desired response time for IaaS.

The pricing strategy of IaaS is based on the cost of servers, storage space, network equipment and system software like operating systems and database systems. The price of IaaS is basically a subscription fee for a specific timeline. Now the question is how to compute this subscription fee. The rate should be fixed based on the cost of hardware and software, target revenue and profit margin. The service provider may adopt a profit maximizing pricing strategy or revenue maximizing pricing strategy within reasonable, stable target profit margin. The profit margin is a dynamic variable; it should be set intelligently according to competitive intelligence and quality of service. The quality of service is measured in terms of computing time. For small firm or individual service consumer, the provider can set a fixed price per unit time; there may be SLA but there is no scope of negotiation of price. Large PSU can negotiate with the service provider to set a rational price for fixed timeline.

Incentive compatibility plays a significant role in IaaS pricing, it is important to analyze the significance of incentives for network infrastructure investment under different pricing strategies: *congestion based negative externality pricing* and the flat *rate pricing*. A lack of proper infrastructure investment incentive may lead to an environment where network growth may not keep pace with the service requirements. It is really complex to compute maximum capacity that IaaS provider will be willing to invest under different pricing schemes. Optimal capacity of IaaS is determined by different factors: per unit cost of capacity of network resources, average value of the user's requests, average value of the user's tolerance for delay and the level of exogeneous demand for the services on the network. It is hard to determine whether time based pricing is more profitable than flat rate pricing. IaaS consumers always try to identify whether average stream of the net benefits realized under congestion based pricing is higher than the average net benefits under flat rate pricing. IaaS provider may adopt different types of pricing strategies at different points of time but the service consumers may control their demand of IaaS service adaptively to avoid the increase in cost.

***Platform-as-a-Service (PaaS)* : PaaS supplies all the resources required to build applications and services completely from the web without any download or installation of any software in the clients. The price of PaaS can be negotiated for a specific project. There can be different types of project environments such as application-delivery-only-environment (e.g. security and on demand scalability), standalone environment and add-on-developmental-environment (e.g. subscriptions of add-on SaaS application are bought). The price of system software can be charged as a subscription fee based on number of concurrent users and usage period. The pricing of PaaS is also governed by the complexity of platform services which may include application design, development, testing, deployment, hosting,**

geographically dispersed team collaboration, web service integration, database integration, security, scalability, storage, state management and versioning. The developers, project managers, and testers can access the development and testing softwares of the service provider through web; but lack of interoperability and portability may be a critical issue in PaaS. The price of PaaS is determined by the complexity of interoperability between the systems of the service provider and service consumer.

Virtual and Augmented Reality **: There are three types of reality technologies: virtual reality (VR), mixed reality (MR) and augmented reality (AR). These reality technologies are sophisticated, creative and powerful tools to offer a complete computerized digital experience through artificial intelligence, computer vision, computer graphics and automation. A virtual entity may not exist physically but created by software in a digital environment. Augmented reality is an enhanced version of the real-world by overlaying our existing reality with an additional layer of digital information, which can be viewed through smartphones or smart glasses (ARSGs). Mixed reality facilitates the merger of and real-time interaction between, digitally rendered and real-world data and objects through MR headset. Virtual reality is characterized by generating real-time, immersive and interactive multi-sensory experiences situated in and artificially induced by a responsive three-dimensional computer-generated virtual environment - usually paired with advanced input and output devices.**

The expert panel are analyzing a smart grid in terms of self-healing network. The basic building blocks of a self healing network are computationally efficient state estimation algorithms that can predict voltage and phase at different nodes of a smart grid in real-time given the current and predicted energy demand and supply of the prosumers. Distributed coordination is important for automated voltage regulators, voltage control and balancing demand and supply during recovery of faults. It is really challenging to develop automated and distributed active network management strategies given the uncertainty of demand and supply at different levels in the smart grid, fault correction mechanisms, self healing strategies, cause-effect analysis on various types of faults (e.g. overload, over current, earth fault, short circuit, over voltage, under voltage, over frequency, under frequency, automatic voltage regulation). An active network configures the topology automatically, sends control signals to individual customers to adjust generation and also load control, automatically correct faults and self-heals the smart grid.

A self-healing mechanism should maintain the stability of a distribution network, perform accurate and timely monitoring and control of the prosumers; big data analysis for multiple actors and sensors, micro-level measurement and predict the future state of smart grid. It can adopt a set of active network management techniques based on distributed intelligence in the self healing network for fast recovery from faults. In case of voltage drift, automatic action is necessary on the transformer to reestablish correct voltage levels. It is essential to balance the mismatch between supply and demand to avoid blackout situation. Essential need of a self healing mechanism is that various components of a smart grid should be able

to communicate for voltage regulation and control of generation capacity and load demand.

Artificial intelligence can be applied to a smart grid in various ways such as knowledge based expert system for knowledge acquisition, inference engine, knowledge base, applications, fault diagnosis; real time alarm handling and fault analysis (AHFA); voltage control such as voltage collapse monitor (VCM), reactive power management (RPM), combined active and reactive dispatch (CARD), power system protection for protective relay setting, phase selection, static security assessment, condition monitoring, scheduling and maintenance of electrical transmission networks and intelligent system for demand forecasting. It is interesting to apply various types of soft computing tools for smart grid system performance analysis. Adaptive fuzzy system is used for fuzzy reasoning, defuzzification and function approximation on imprecise and uncertain data. Artificial neural network can be useful for intelligent data mining, neuro-fuzzy control, neuro expert power system and evolutionary computing (e.g. neuro GA).

Let us do technical analysis on evolution of AI in a smart grid system. A knowledge based expert system captures the knowledge of human expert in a specific domain. It uses the knowledge for decision making and appropriate reasoning of complex problems. The expert system needs a knowledge structure in the form of production rules, frames and rules. A knowledge base is a form of database containing both facts and rules. Let us present here examples of few rules.

- **Rule 1 : If X = True, Then Y= True.**
- **Rule 2 : If X= True and Y= True then Z= True.**
- **Rule 3 : IF I is An isolator AND current through I is 0 AND I = closed**
    - **THEN open I.**
- **Rule 4: AND Rule - A.B = X.**
- **Rule 5 : NAND Rule - NOT (A.B) = NOT (X).**
- **Rule 6: OR rule - A+B = Y.**
- **Rule 7 : NOR rule - NOT (A + B) = NOT (Y).**
- **Rule 8 : XOR rule - A ⊕ B = Z /* NOT (A). B + A. NOT (B) = Z*/**

An expert system (ES) can function based on knowledge of power system operation which may or may not be complete. An ES performs several functions such as knowledge acquisition and inference engine [16]. Data mining algorithms analyze SCADA data. This component acquires new facts or rules. Inference engine performs several functions such as verification, validation, cause-effect analysis, sequence control for rule firing, data processing, meta knowledge management, forward and backward chaining. But, ES may have some limitations from the perspectives of inappropriate representation of knowledge structure. Expert systems can be used in power system analysis

- **Planning : AC/DC network design, power plant management, capacity planning;**
- **Operation: alarm processing, fault diagnosis, forecasting. Maintenance scheduling, demand side management, reactive voltage control;**
- **Analysis : Control system design, power system protection and coordination;**
- **AC load flow analysis : Input data includes network parameters, connections, loads, maximum active and reactive power output. It minimizes a set of**

objective functions subject to a set of constraints such as network laws, plant loading limits, busbar voltage limits, line loading constraints and security.

Case : Self-healing smart solar grid

North American power grid, one of the greatest engineering innovations of 20th century is now 50 years old and needs a smart self healing grid to incorporate renewable energy sources, reduced number of power outages and reduced carbon emissions [44]. North America has already experienced a number of power outages. In 2012, the occurrence of hurricane Sandy caused power outages in twenty four state of USA and shut down of schools and offices. In 2003 a blackout occurred for two days throughout North-eastern and Midwestern parts of USA and United States and the Canadian province of Ontario. The cause of the blackout was a software bug in the alarm system at a control room of the First Energy Corporation in Ohio. In 2011, New England experienced a Halloween snowstorm that put millions of people in the dark for several days. The following section presents a self healing mechanism [SHM] for the smart power grid.

Self Healing Mechanism [SHM]

Agents **: Service consumers (B)[e.g. smart home, smart building, industrial load, solar pump for agriculture, microgrid], Service provider (S);**

Structure

- **Smart power grid comprising of power generation, transmission and distribution system, generators, transformers, transmission lines, loads, switchyards, microgrids comprising of AC / DC sources and loads, renewable energy sources (e.g. PV panels) and energy storage system;**
- **fully automated power delivery network that monitors and controls a set of nodes, supports a bidirectional flow of electrical power and information among the power plants, loads and all intermittent points;**

Scope:

- **ensure stability, reliability, consistency and improved efficiency during normal operating conditions;**
- **self-recovery during human error or natural disaster;**
- **enable better integration between conventional grid and renewable energy sources;**
- **mitigate the impact of power outages;**
- **ensure fewer blackouts for shorter periods;**
    - **maintain the stability of the smart grid;**
    - **perform accurate and timely monitoring and control of the prosumers;**
    - **big data analysis for multiple actors and sensors through micro-level measurement;**
    - **predict the future state of smart grid;**
    - **fast recovery from faults;**

        - automatic action on the transformer to reestablish correct voltage levels in case of voltage drift
        - balance the mismatch between supply and demand to avoid blackout situation
        - various components of a smart grid should be able to communicate for voltage regulation and control of generation capacity and load demand;
- **Constraints : time, cost, technology;**

Strategy: Select a set of intelligent strategic moves rationally.

    - **Call deep analytics : '7-S' model**
    - **Automated model checking and system verification**
    - **Real-time smart grid monitoring; adaptive and resilient approach in fault analysis and fault clearing**
    - **Adoption of self-stabilizing and self-organizing distributed network management strategy**
    - **Digital power system protection system for giving alarm / alert in time, voltage and reactive power control**
    - **SWOT analysis : AI enabled smart grid has more benefits in terms of cost, flexibility and**
    - **TLC analysis /* AI enabled smart grid is at growth phase of S-curve today */.**

System **: AI enabled expert system**

- **Input : Demand plan of B, Supply plan of S;**
- **Output : Energy contract;**
- **Protocol:**
    - **define and configure expert system in the form of knowledge base, knowledge acquisition system, inference engine, workplace or memory, justifier, user interface, knowledge refining system and consulting environment;**
    - **develop self-stabilizing and self-organizing distributed network management algorithms;**
    - **call computationally efficient state estimation algorithms that can predict voltage and phase at different nodes of a smart grid in real-time given the current and predicted energy demand and supply of the prosumers;**
    - **distributed coordination for automated voltage regulators, voltage control and balancing demand and supply during recovery of faults;**
    - **automated and distributed active network management strategies given the uncertainty of demand and supply at different levels in the smart grid, fault correction mechanisms, self healing strategies, cause-effect analysis on various types of faults;**
    - **Configuration of the network automatically, sends control signals to individual customers to adjust generation and also load control, automatically correct faults and self-heals the smart grid.**

Security

- **verify *security intelligence* through automated or semi-automated system verification.**
    - **Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities.**
    - **call threat analytics and assess risks on smart grid; analyze performance, sensitivity, trends, exception and alerts.**
    - **what is corrupted or compromised: agents, communication schema, data schema, application schema and computing schema ?**
    - **time : what occurred? what is occurring? what will occur? assess probability of occurrence and impact.**
    - **insights : how and why did it occur? do cause-effect analysis.**
    - **recommend : what is the next best action?**
    - **predict : what is the best or worst that can happen?**
- **Verify security intelligence of a smart grid at various levels such as L_1, L_2, L_3, L_4 and L_5.**
    - ***Level L_1* verifies system performance in terms of stability, reliability, consistency, safety, liveness, robustness, resiliency, deadlock-freeness and synchronization.**
        - ***Unsymmetrical fault analysis***
            - ***Shunt type faults***
                - ***Line-to-Line fault***
                - ***Single Line-to-Ground fault***
                - ***Double Line-to-Ground fault***
            - ***Series type faults***
                - ***Open conductor fault***
        - ***Symmetrical fault analysis***
        - ***Smart grid stability analysis***
            - ***Transient stability***
            - ***Steady state stability***
            - ***Voltage stability analysis***
        - ***Smart grid security analysis***
            - ***Contingency analysis***
            - ***Sensitivity analysis***
    - ***Level L_2* verifies access control in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, trust and commitment of the users and system administrator.**
    - ***Level L_3* verifies computing schema in terms of fairness, correctness, transparency, accountability and accuracy of measurement of data.**
    - ***Level L_4* verifies the efficiency of digital relay protection such as overload, over current, earth fault, short circuit, over voltage, under voltage, over frequency, under**

frequency, automatic voltage regulation, reactive power control and distance protection;

- ***Level L_5*** **assesses the risks of various types of malicious attacks on a smart grid such as denial of service (DoS), sybil attack, false data injection attack and coremelt attack.**
- ***Revelation principle*** **: B and S preserve privacy of energy contract as per revelation principle;**

Staff-Resources **: system administration, technical, management, operation, maintenance;**

Skill-Style-Support **:**

- **intelligent coordination and integration among 7-S elements**
- **Proactive and preventive support**
- **Reactive support**

Payment function**:**

- **The agents settle single or multiple intelligent service contracts.**
    - **Collaborative planning, forecasting and replenishment (CPFR)**
    - **Swing option**
    - **verify business intelligence of service contracts in terms of (pay per use, payment mode, payment terms).**

A smart self-healing grid is a sophisticated electrical platform that is expected to ensure stability, reliability, consistency and improved efficiency during normal operating conditions; self-recover during human error or natural disaster and enable better integration of renewable energy sources. A self-healing grid should be able to mitigate the impact of power outages during polar vortex, flood, cyclone or snow storm and must ensure fewer blackouts for shorter periods. Self-stabilization and self-organization are two important properties of a self-healing smart grid. Availability, robustness and the possibility for on-demand reconfiguration of distributed complex systems are important in various types of applications such as self-healing smart grid, dynamic sensor network and communication network. A smart grid is expected to be a self-stabilizing system that reaches an arbitrary inconsistent state due to the occurrence of transient faults but can recover automatically from such faults and converge to a desired state. It is not only applicable to a large, distributed and heterogeneous smart grid but also to routing algorithms in communication networks.

Is it possible to adopt collaborative planning, forecasting and replenishment (CPFR) as a strategic tool for comprehensive value chain management of a group of trading agents associated with the smart grid? It may be an interesting initiative among all the stakeholders of the smart grid in order to improve their relationship through jointly managed planning, process and shared information. The interplay between trust and technology encourages the commitment of collaboration among the trading agents.

Let us consider a specific scenario of multi-party negotiation in trading of smart grid. Swing option is a specific type of supply contract. It gives the owner of the

swing option the right to change the required delivery of a resource through short time notice. It gives the owner of the swing option multiple exercise rights at many different time horizons with exercise amounts on a continuous scale. A typical swing option is defined by a set of characteristics and constraints. There are predefined exercise times t_i, i ∈[1,2,..,n], 1≤ t_1≤t_2…≤t_n≤ T at which a fixed number of $d_0$units of a resource may be obtained. With a notice of specific short period, the owner of the option may use swing right to receive more (up-swing) or less (down-swing) than d_0 at any of n moments. The scheme permits swing only at g out of possible n time moments where g ≤ n is swing number constraint. A freeze time constraint forbids swings within short interval of the moments. The local constraints up-swing [α] and down-swing limits [β] define how much the requested demand d_i at time t_i may differ from d_0.

There are two global constraints which restrict the total requested volume D within the contract period by maximum total demand (γ) and minimum total demand (λ). The option holder must pay penalty determined by a function for violating local or global constraints. In this contract, the primary negotiation issue may be a discriminatory pricing plan which depends on the negotiation of a set of secondary issues such as up-swing limit, down-swing limit, maximum total demand, minimum total demand, penalty function and number of swings for a specific period.

Self-stabilization is well defined but self-organization property is not. Self-organization satisfies locality and dynamicity. A smart grid is self-organizing if the distributed algorithm associated with it converges or stabilizes in sub-linear time with regards to the number of nodes and reacts fast to the changes of the topology of the distributed network. The addition and removal of nodes influences a small number of states of other nodes of the distributed network. If s(n) is upper bound on the convergence time and d(n) is upper bound on the convergence time following a change in topology, then s(n) ∈ o(n) and d(n) ∈o(s(n)). The algorithm converges in O(log n) expected number of rounds, responds to dynamic changes locally and is therefore self-organizing.

In a distributed smart grid, it is hard to predict in advance the exact combination of failures and the systems require intelligent and complex coordination mechanisms among the processors, computers and communication networks. A distributed system can be modeled by a set of n state machines or processors ($P_{i,i=1,\ldots,n}$) which communicate with other neighbors. A distributed smart grid can be represented by a graph G = (V,E) in which each processor is known as node and each two neighboring nodes are connected by a link of the graph. Each node runs a program and changes state with execution of each executable program statement.

Self-stabilization in solar computing **: Is it possible to imagine the smart grid as a complex graph in solar computing system? Let us consider a unidirected graph G = (V,E) to represent the system associated with the smart grid, each processor p_i is represented by a vertex v_i ∈ V and each communication link used for transferring data from p_i to p_j is an edge (i, j) ∈ E; opposite directed edge (j, i) ∈ E; the number of edges linked to a node is bounded by a constant. The distance between two processors p and q is dist(p, q), the shortest path between p and q in the graph.**

Overlay edge denotes a path of edges that connects two processors in the system. When the path is predefined and fixed, it acts as a virtual link where a processing time is required by intermediate processors to forward the data from source to destination. We regard the time it takes a message to traverse such an overlay link as the time for traversing a link that directly connects two neighboring processors. A configuration c of the system is a tuple c = (S,L); S is a vector of states, s_1, s_2, · · · s_{ni}, where the state s_i is a state of processor p_i; L is a vector of *link states.* A processor changes its state according to its transition function. A transition of processor p_i from a state s_j to state s_k is called a *step* and is denoted by a. A step a consists of local computation and of either a single send or a single receive operation. An *execution* is a sequence of global configurations and *steps*, E = {c_0, a_0, c_1, a_1, . . .}, so that the configuration c_i is reached from c_{i-1} by a step a_i of one processor p_j. The states changed in c_i, due to a_i, are the one of p_j and possibly that of a link attached to p_j . The content of a link state is changed when p_j sends or receives data during a_i. An execution E is *fair* if every processor executes a step infinitely often in E and each link respects the bounded capacity loss pattern. In the scope of self-stabilization, we should consider executions that are started in an arbitrary initial configuration. A *task* is defined by a set of executions called *legal executions* and denoted LE. A configuration c is a *safe configuration* for a system and a task LE if every fair execution that starts in c is in LE. A system is self-stabilizing for a task LE if every infinite execution reaches a safe configuration with relation to LE. The algorithm stabilizes if it has reached a safe configuration with regards to the legal execution of the corresponding task.

Smart grid security analysis

***Unsymmetrical fault analysis* : The majority of system faults are not 3 phase symmetrical faults but the faults involving shunt types faults (e.g. Line-to-Line fault, double Line-to-Ground fault and and series types faults (e.g. open conductor fault). Can a solar grid face such types of unsymmetrical faults for both single and three phases system? What are the countermeasures? Unsymmetrical system operation often results unsymmetrical faults Under unbalanced conditions, the system impedance in each phase may not be identical; three phase voltages and currents throughout the system may not be completely balanced i.e. may not have equal magnitude in each phase and are not displaced in time phase correctly. System operation and loads may be unbalanced. Unsymmetrical faults are generally analyzed through symmetrical components wherein three phase unbalanced voltages and currents may be unbalanced and transformed into three sets of balanced voltages and currents.**

***Symmetrical fault analysis*: This is the analysis of abnormal behavior of a smart grid under the conditions of symmetric short circuit 3 phase faults due to various reasons such as insulation failure of power system equipments or flashover of lines due to lightning strike or accidental faulty operation.. The smart grid must be protected against flow of heavy short circuit current by disconnecting faulty system through circuit breakers operated by protective relays. Symmetric fault is rare but the**

analysis is crucial to protect a smart grid against the flow of most severe fault current. Can a solar grid face such type of symmetrical faults? What are the countermeasures?

Smart grid stability analysis **: The stability of a smart grid is the ability of an interconnected power system to return to normal or stable operation after some form of disturbance due to loss of synchronization or falling out of step. Stability analysis is an essential part of smart grid planning, coordination and integration among various components of power system. The stability of a smart grid may be classified into steady state, dynamic and transient; is it valid for a solar grid? The study of steady state stability is the determination of upper limit of machine loading before losing synchronism provided the loading is increased gradually. The steady state stability limit of a smart grid is the maximum power that can be transmitted to the receiving end without loss of synchronism. It is crucial to know the steady state limit to improve the stability limit of the grid. Dynamic stability is more probable than steady state instability. Small disturbances occur continuously in a smart grid. The grid is dynamically stable if the oscillations do not acquire more than certain amplitude and die out quickly? Transient stability is the impact of sudden large disturbance of power system on various components of smart grid due to the occurrence of opening or closing power generation units, tripping of a loaded generation unit, abrupt dropping of a large load or fault on a heavily loaded line. It is also crucial to determine the effects of short circuit faults, the most severe type of disturbances on a solar grid. The stability of the solar grid may depend on various factors such as type and location of fault, rapidity and method of fault clearing (e.g. sequential or simultaneous opening of circuit breakers or isolators). A practical approach to transient stability analysis is to list all important severe disturbances along with their possible locations in the grid. The grid may be stable on occurrence of a fault or may be stable if the fault is cleared in time. A smart grid may be associated with multiple generation units and load. Computer simulation is an effective method of stability analysis of complex multi-machine system associated with a solar grid. A digital computer programme can compute the system parameters due to transients for effective system control. Another critical issue is to improve the transient stability of solar grid through various ways such as use of high speed reclosing circuit breakers, reduction in system transfer reactance, use of high speed excitation system and increasing system voltage.**

Voltage stability **is the ability of a smart solar grid to maintain acceptable voltages at all buses in the system under normal conditions and after being subjected to disturbance. The grid may lose stability when a disturbance results a progressive and uncontrollable decline in voltage. Inadequate reactive power support from generation units and transmission lines leads to voltage instability, voltage collapse and may result blackout. Voltage stability may be ensured by raising the terminal voltage of generation unit, tap value of generation transformer, Q-injection, load end OLTC and strategic load shedding. It is essential to ensure voltage security in terms of the ability of a system, not only to operate stably but also to remain stable following any reasonably credible contingency or adverse system change such as increase in load. It is essential to perform voltage stability analysis of a smart solar**

grid though the study of load flow based static and system dynamics analysis in terms of various parameters such as small and long disturbance voltage stability, stable voltage, voltage collapse, transient voltage and voltage security.

***Security analysis : S*ecurity constrained optimization is essential to ensure secure and economical operation of a smart grid. The grid may face emergency condition based on the severity of violations of operating limits. The grid must withstand the effects of contingencies to avoid heavy overloading of system components, cascading failure and system blackout. If the process of cascading failure continues, the grid as a whole or its major parts may completely collapse. System security analysis is carried out in computerized energy control centres in terms of system monitoring, contingency analysis and corrective action analysis. The basic objective of system monitoring is to give the best estimate of current system conditions or states of the smart grid through SCADA (Supervisory Control & Data Acquisition System). The basic objective of contingency analysis is to carry out emergency identification and what-if simulation; prediction of possible system outages before the occurrence and give alert against potential overloads and / or voltage violations. Corrective action analysis provides preventive and post contingency control and permits the system administrators to change the operation of the power system if contingency analysis predicts a serious problem in occurrence of a certain outage.**

Contingency analysis is normally performed in three distinct states : contingency definition, selection and evaluation. Contingency definition gives the list of contingencies to be processed where the probability of occurrence is high. Contingency selection ranks a set of contingencies as per the order of severity using direct and indirect method. Contingency evaluation is performed in decreasing order of severity and is continued upto the point where no post contingency violations are encountered. The security control is achieved through security constrained optimization program. It is necessary to ensure the reliability of the smart grid so that adequate amount of power is generated and distributed with enough redundancy so that the grid can withstand all major failure events. Another critical issue is sensitivity analysis to compute possible overloads based on generation shift factors and line outage distribution factors.

In this session, the panel have considered the technology of IIoT enabled Industrial Control System (ICS) and SCADA configured with computers, electrical, electronic and mechanical equipments; operated in automated or semi-automated operation mode and used in manufacturing and chemical plants, power plants, energy and utilities distribution, communication and transportation systems. ICS interacts with the physical environment and is associated with a complex information system. ICS integrates computing, networking, data, application and security schema, sensors and actuators. ICS may be threatened by cyber and other various types of malicious attacks; safety, reliability, consistency and fault tolerance are critical issues.

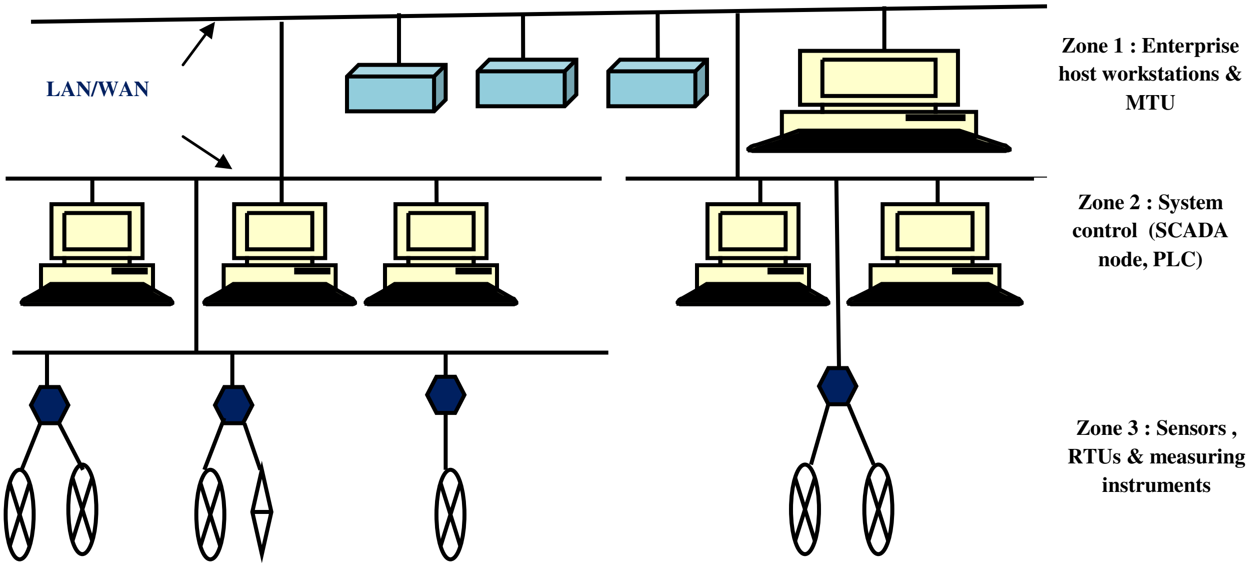

LAN/WAN
Zone 1 : Enterprise host workstations & MTU
Zone 2 : System control (SCADA node, PLC)
Zone 3 : Sensors , RTUs & measuring instruments

Figure 10.2 : ICS / SCADA Architecture

In general, ICSs can be simple, medium and very complex systems which may include thousands of different components distributed over different zones and controlling real-time complex processes. Industrial Control Systems can be broadly segmented into three different zones such as Enterprise, Control and Field zone (as per IEC TS 62443-1-1 2009) [Figure 10.2]. The enterprise zone includes business networks and enterprise systems; the control zone includes various control elements; the field zone includes the devices (e.g. PLC) and networks used for automation. A plant may have different segments such as power generation, transmission, and distribution and metering. Next, let us focus on networking schema of ICS/ SCADA architecture. Typically, several wireless technologies can be used for ICS / SCADA such as Wireless Local Area Network (WLAN) and Bluetooth (as per open IEEE 802.15.1 standard; operates in 2.4 GHz ISM band). Various components of an ICS / SCADA can communicate with each other through a set of protocols such as IEEE 802.11x, Bluetooth, cellular, Wireless HART, ISA 100.11a, Z-Wave, Zigbee, Microwave and satellite technologies.

Let us discuss IoT enabled SCDA & ICS. Due to recent innovation of internet connectivity, digital and smart manufacturing technologies, IoT has become a revolutionary technology. The applied domains include supply chain management, transport, utilities, industrial automation, healthcare, building and home automation. IoT is an emerging technology that connects physical objects, internet and communicate with one another (similar to HCI). IoT connects systems, sensors and actuators to the internet. Physical objects + Sensors, actuators and controllers + Internet = IoT (Connect, communicate and data exchange). Another emerging trend of SCADA & ICS is IIoT; this includes real-time monitoring and process control like real-time optimization of production and supply chain networks in manufacturing industry; deployment of smart machines, sensors and controllers with proprietary communication and internet technologies, automated process

control using digital controllers to achieve enhanced productivity and safe distribution system; maximizing safety, sensitivity, security and reliability through high precision automation and control. What is the scope of IoT for electric power system? It includes smart metering, AMI (Advanced Metering Infrastructure), connected public lighting, smart inverters, plant, SCADA, remote control operation of energy consuming devices, home entertainment (audio, video, projectors), smart lighting adapting ambient conditions based switching, wireless internet connected lights, smoke and gas detection, smart appliances, management and control, intrusion detection and surveillance system.

SMQC Algorithm

Agents: **Client (C), Database Administrator (A); /* C and A may be automated agents.*/**

System **: Private database (SDB);**

Input **: Query (q);**

Output**: Response (r);**

Procedure**:**

1. C challenges A → sends query (q).

2. A retrieves response (r) from SDB.

3. A selects correct move to preserve privacy of r.

- ⊕ ***Suppress r partially.***
- ⊕ ***Perturb r by randomization.***
- ⊕ ***Achieve k-anonymity through generalization / suppression / de-identification of r.***
- ⊕ ***Summarize or aggregate r.***
- ⊕ ***Replace r with a small sample.***
- ⊕ ***Partition r.***
- ⊕ ***Swap r.***
- ⊕ ***Audit r.***

4. **A applies quantum signcryption algorithm on r and sends signcrypted r to C.**

5. C unsigncrypts r w.r.t. q → verifIies correctness and data integrity of r.

+

Theorem **:** ***SMQC algorithm preserves the privacy of data through a set of information disclosure control method and signcryption of critical data.***

Quantum computing is a promising technology to solve computation problems significantly faster as compared to classical computers. This technology is based on the concepts of quantum mechanical phenomena such as superposition and entanglement to process data efficiently. Quantum theory analyzes the nature of energy and matter on the atomic and subatomic level. Quantum computing is a branch of quantum information science (e.g. quantum cryptography, quantum communication). In a classical computer, Boolean logic is represented through a set of bits where each bit is either 1 or 0. Quantum computers are not limited to two states and encode information as quantum bits. Qubits are the basic building blocks of quantum computing. Qubits can be in a 1 or

0 quantum state; can also be in a superposition of 1 and 0 states. When qubits are measured, the result is always either 0 or 1; the probabilities of the two outcomes depend on the quantum state of the qubits. Qubits represent atoms, ions, photons or electrons that work together to act as computer memory and a processor. It is rational and an interesting research agenda to understand the consequences of quantum technologies in the context of secure multi-party computation. Is it possible to construct secure multiparty computation protocols against quantum attacks? How to preserve privacy in secure multi-party quantum computation by optimizing quantum computational power, space and time complexity. Is it possible that dishonest parties gain no information about the private inputs of honest agents in secure quantum computing setting? Is it possible to ensure fairness and correctness in secure multi-party quantum computing : if the parties do not abort the protocol, then at the end of the protocol they share a state corresponding to the correct computation applied to the inputs of honest parties and some choice of inputs for the dishonest parties ?

Distributed computing considers the scenario where a number of distinct, yet connected computing agents wish to execute a joint computation. The objective of secure multi-party computation is to enable these agents to carry out such distributed computing tasks in a secure manner. The advancement of computer network technologies, multiagent system and cryptography has improved the efficiency of secure multi-party computation significantly. Let us define *Secure Multi-party Quantum Computation.* Two or more agents want to conduct a computation based on their private inputs but neither of them wants to share its proprietary data set to other. The objective of secure multiparty computation is to compute with each party's private input such that in the end only the output is known and the private inputs are not disclosed except those which can be logically or mathematically derived from the output. In case of secure multi-party computation, a single building block may not be sufficient to do a task; a series of steps should be executed to solve the given problem. Such a well-defined series of steps is called SMC protocol. It has some useful properties - privacy, correctness, independence of inputs, guaranteed output delivery and fairness. A protocol ensures correctness if each party receives correct output. Corrupted (or malicious) parties select their inputs independently of the inputs of honest parties and honest parties must receive their output. Corrupted parties should receive their outputs if and only if the honest parties receive their outputs and this ensures fairness of the protocol.

In the study of SMC problems, two models are commonly assumed : semi-honest and malicious model. A semi-honest party follows the protocol properly with correct input. But after the execution of the protocol, it is free to use all its intermediate computations to compromise privacy. A malicious party does not need to follow the protocol properly with correct input; it can enter the protocol with an incorrect input. A third party may exist in a protocol. A trusted third party is given all data; it performs the computation and delivers the result. In some SMC protocols, an untrusted third party is used to improve efficiency.

A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. Secure multi-party computation preserves privacy of

data in different ways; is it possible to apply following methods for secure multi-party quantum computing model? What are the algorithms? is the cost of computation and communication high in case of quantum computing? It is rational to apply following methods on the original data first and then apply quantum cryptographic algorithms (e.g. signcryption, encryption) on the perturbed data.

- ***Add random noise to data* : The basic objective of data perturbation is to alter the data so that real individual data values cannot be recovered. For an input x, (x+r) preserves the privacy of x if r is a secret random number.**
- ***Split* a data or message into multiple parts randomly and sending each part to a DMA through a number of parties hiding the identity of the source,**
- ***Control the sequence of passing* selected data or messages from an agent to others through serial or parallel mode of communication.**
- ***Dynamically modify the sequence of events* and agents through random selection.**
- ***Permute* the sequence of messages randomly.**
- ***Masking***

In SMQC algorithm as stated above, the client (C) interacts with the system administrator (A) through enterprise applications or web; submits simple or complex queries and searches for intelligent information. A malicious agent may be able to attack the server during this communication between C and A. SMQC tries to protect sensitive data from unsolicited or unsanctioned disclosure of data by calling different information disclosure control methods such as suppression, perturbation, randomization, k-anonymity through generalization or de-identification, summarization or aggregation, data partitition and data swap. The privacy of sensitive data may be preserved by suppressing the data intelligently before any disclosure or computation. Specific attributes of particular records may be suppressed completely. In case of partial suppression, an exact attribute value is replaced with a less informative value by rounding or using intervals. K-anonymity is achieved through generalization, suppression and de-identification. The attribute values are generalized to a range to reduce the granularity of representation. Quasi-identifier attributes are completely or partially suppressed. De-identification is achieved by suppressing the identity linked to a specific record or altering the dataset to limit identity linkage. Summarization releases the data in the form of a summary that allows approximate evaluation of certain classes of aggregate queries while hiding individual records. The sensitive data set may be replaced with a small sample. Aggregation presents data in the form of sum, average or count. Randomization perturbs the data randomly before sending them to the server and introduces some noise. The noise can be introduced by adding or multiplying random values to numerical attributes. The system administrator generally preserves the privacy of sensitive data through signcryption. C checks whether different statistical disclosure control tools are really able to preserve the privacy of sensitive data from the adversaries during communication.

It may be possible to restrict the query of the client through various ways such as query set size control, query set overlap control, auditing, cell suppression, data swap and data patitioning. The query set size control method permits information

w.r.t. a query be released only if the size of the query set satisties specific condition.Auditing keeps up-to-date logs of all queries made by a client and checks constantly possible compromise whenever a new query is issued. Auditing provides the client with unperturbed response if the response does not compromise privacy of critical information. Bit, audit may require high cost of data processing time and storage requirements. The basic objective of partitioning is to cluster individual entities of the population in a number of mutually exclusive subsets or atmic populations. The basic objective of suppression is to restrict the disclosure of confidential information by suppressing a specific set of cells of a data schema. Data perturbation may have probability distribution and fixed data perturbation strategy. The first method extracts a sample from the population with a probability distribution. In the second category, the values of specific attributes are perturbed once and for all. Another interesting method is approximate data swap of multicategorical attributes of data schema.

Privacy is the primary concern of secure multi-party quantum computing; is it possible to address the issue utilizing the concept of cryptography and secure multiparty computation? The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption methods. The sender (S) encrypts a message (m) with encryption key and sends the cipher text (c) to the receiver (R). R turns c back into m by decryption using secret decryption key. In this case, an adversary may get c but cannot derive any information. R should be able to check whether m is modified during transmission. R should be able to verify the origin of m. S should not be able to deny the communication of m. There are two types of key based algorithms - symmetric and public key. Symmetric key encryption scheme provides secure communication for a pair of communication partners; the sender and the receiver agree on a key k which should be kept secret. In most cases, the encryption and decryption key are same. In case of asymmetric or public-key algorithms, the key used for encryption (public key) is different from the key used for decryption (private key). The decryption key cannot be calculated from the encryption key at least in any reasonable amount of time. The widely-used public–key cryptosystem are RSA cryptosystem (1978), Elgamal's cryptosystem (1985) and Paillier's cryptosystem (1999). The challenge is how to apply existing encryption and decryption algorithms in quantum computing : is it possible to perform quantitative operations of quantum computing on encrypted data? How?

Is it possible to apply *digital signature* for secure multi-party quantum computing model? A digital signature is a cryptographic primitive by which a sender (S) can electronically sign a message and the receiver (R) can verify the signature electronically. S informs his public key to R and owns a private key. S signs a message with his private key. R uses the public key of S to prove that the message is signed by S. The digital signature can verify the authenticity of S as the sender of the message. A digital signature needs a public key system. A cryptosystem uses the private and public key of R. But, a digital signature uses the private and public key of S. A digital signature scheme consists of various attributes such as a plaintext message space, a signature space, a signing key space, an efficient key generation

algorithm, an efficient signing algorithm and an efficient verification algorithm. There are various forms of digital signature such as group signature and ring signature. A group signature scheme allows a member of a group to sign a message anonymously on behalf of the group. A designated entity can reveal the identity of the signer in case of any dispute. The challenge is how to apply existing digital signature algorithms in quantum computing : is it possible to perform quantitative operations of quantum computing on digitally signed data? How?

Is it possible to apply *signcryption* for secure multi-party quantum computing model? Traditional signature-then-encryption is a two step approach. At the sending end, the sender signs the message using a digital signature and then encrypts the message. The receiver decrypts the cipher text and verifies the signature. The cost for delivering a message is the sum of the cost of digital signature and the cost of encryption. Signcryption is a public key primitive that fulfills the functions of digital signature and public key encryption in a logically single step and the cost of delivering a signcrypted message is significantly less than the cost of signature-then-encryption approach. A broadcasting system is vulnerable to insecure communication. The basic objective is that the system properly signcrypts all sensitive data. A pair of polynomial time algorithms (S,U) are involved in signcryption scheme where S is called signcryption algorithm and U is unsigncryption algorithm. The algorithm S signcrypts a message m and outputs a signcrypted text c. The algorithm U unsigncrypts c and recovers the message unambiguously. (S,U) fulfill simultaneously the properties of a secure encryption scheme and a digital signature scheme in terms of confidentiality, unforgeability and nonrepudiation. Signcryption can ensure efficient secure communication. The basic objective is to provide confidentiality, data integrity, authentication and non-repudiation in the communication of sensitive data. The challenge is how to apply existing signcryption and unsigncryption algorithms in quantum computing : is it possible to perform quantitative operations of quantum computing on signcrypted data? How?

System Analytics : Secure Adaptive Filter Mechanism (SAFM)
***Agents*: System analysts;**

- ***Scope* :**
    - **Spam filtering**
    - **Web caching - DoS attack prevention in cache miss**
    - **Distributed systems, networking applications, database applications, data streaming algorithms**
  - **Constraints: space and time complexity;**
- ***System*: Adaptive filter in adversarial environment;**
    - ***Adaptive Filter (Type 1) /* Private search mechanism */***
        - ***Input*: A secure adaptive filter represents a set S of elements approximately.**
        - ***Lookup*: Given an element x, the buckets given by $h_i(x)$ are examined to see if x is in the list i.e. data schema.**
        - ***Insertion*: Given an element, first check that x is not already in the list via a lookup. If not, sequentially**

examine the buckets $h_i(x)$. If there is empty space, x is inserted into the first available space. If no space is found, a value j is chosen independently and uniformly at random from [1; d], and x is stored in the jth sublist at bucket $h_j(x)$. It displaces an element y from that bucket and then insertion is recursively executed for y.

      - *Deletion*: Given an element x, x is searched via a lookup; if it is found it is removed; selectively remove false positive without introducing false negative.
      - *Output*: for any $x \in S$, the filter always answers ‘Yes’ and for any $x \notin S$ it answers ‘Yes’ only with small probability;
    - *Hybrid Adaptive Filter (Type 2)* /* Private search and classification */
      - *Input*: a set S of elements approximately.
      - *Lookup*: Given an element x, the buckets given by $h_i(x)$ are examined to see if x is in the list.
      - *Insertion* /* same as type 1 filter*/
      - *Deletion* /* same as type 2 filter */
      - Call private *optimal margin classifier*. / * refer section 3.1*/
      - *Output*:
        - for any $x \in S$, the filter should always answer ‘Yes’;
          - determines class of $x \in C_i$; /* C_i : i^{th} class */
        - for any $x \notin S$ it should answer ‘Yes’ only with small probability;
- *Structure*: Select right structure based on objective of filter - *Adaptive Bloom filter / Adaptive Cuckoo filter / Parallel pipeline*
- *Security*: call intelligent threat analytics, verify security intelligence at multiple levels.
  - *Level 1*: audit computational intelligence in terms of correctness of computation and rationality of filter configuration,
  - *Level 2*: verify system performance of the adaptive filter in terms of reliability, consistency, resiliency and liveness;
  - *Level 3*: malicious attacks – verify the risks of Denial of Service (DoS), false data injection, intrusion and Sybil attack on adaptive filter;
  - *Level 4*: multi-party corruption - assess the risks of corruption of system administrator and filtering mechanism of adaptive filter;
  - *Level* 5: verify the efficiency of access control of adaptive filter in terms of authentication, authorization, correct identification, privacy, audit, nonrepudiation, confidentiality and data integrity.
    - *Revelation principle* : Preserve privacy of output of adaptive filter.

- ***Strategy / Moves*: Adaptive security, private search, Cuckoo hashing;**
- ***Staff-resources*: Creative talent for K-A-B-C-D-E-T-F innovation model on development of secure adaptive filter;**
- ***Skill-style-support*: Data Structure, Optimal margin classifier, Secure Multi-party Computation;**

***Analysis of SAFM*: An adversary may pick the inputs but gets no information about the randomness of data structure. An adversarial model allows an adversary to choose inputs and queries adaptively according to previous response. With high probability over internal randomness of data structure, the ouput will be correct if an adversary chooses a sequence of inputs adaptively. A secure adaptive filter (e.g. Bloom filter) exists in an adversarial model if one way function exists. Bloom filters use significantly less memory and have very fast query time. These filters are used in distributed systems, networking and database applications, spam filtering, web caching, data straming algorithms and information security.**
U: Large universe; S: A set of elements from U; x: input query to be answered by a secure adaptive filter; For any Output: for any x $\in$ S, the filter should always answer 'Yes' ; For any x /$\notin$ S it should answer 'Yes' only with small probability. What happens if an adversary chooses the next query according to the responses of previous query? Does the bound on the error probability still hold? Under the adversarial model, secure adaptive filters are resilient to spam filtering and web caching attacks by efficient and computationally bounded adversaries.
The security of an adversarial resilient filter can be defined through a security game with an adversary. An adversary is allowed to make a sequence of t adaptive queries to the adaptive filter and gets their responses. The adversary has only oracle access to the filter and can not see the internal memory representation. The adversary must output an element x*as a false positive. A filter (n,t,e) is adversarial resilient if when initialized over sets of size n, then after t queries, the probability of x* being a false positive is at most e. If a filter is resilent for any polynomiallymany queries, it is strongly resilent.

An adaptive filter consists of two algorithms (i) an initialization algorithm that gets a set and outputs a compressed representation of the set. (ii) a membership query algorithm that gets a representation and an input. An adaptive secure filter has a randomized algorithm but a deterministic query algorithm
Security game :
Notation : U- universe of elements; size of U : u;
S : Subset of U, S$\in$U, size of S :n; n$\geq$ log log u;
An adaptive filter is a data structure that is composed of two algorithms, B= (B_1,B_2);
B_1 : Randomized set up algorithm; gets as input a set S and outputs a compressed representation of it B_1(S) =M.
B_2 :Query algorithm; it answers membership queries to S given compressed representation M. It is deterministic and can not change the representation. B_2 is a deterministic algorithm that gets as input representation and a query element x $\in$U. B is (n.t.e) adaptive filter with a steady representation for any set S$\in$U of size n if it holds.

a) completeness : for any x S, $\Pr[B_2(B_1(S),x) = 1] = 1$

b) soundness: for any $x \in S$, $\Pr[B_2(B_1(S),x)=1] \leq e$

False positive : Given a representation M of S, if $x \notin S$ and $B_2(M,x) = 1$, x is false positive; e is the error rate of B

A single fixed input x and the probability is taken over the randomness of B. We want to give a stronger soundness requirement that considers a sequence of inputs $x_1, x_2, \ldots, x_t$ that is not fixed but chosen by an adversary, where the adversary gets the responses of previous queries and can adaptively choose the next query accordingly. If the adversary's probability of finding a false positive x* that was not queried before is bounded by e, then B is an (n, t, e)-resilient Bloom filter setup phase of the Bloom filter and the adversary get the security parameter λ .

Adversarial-resilient Bloom filter with a steady representation: Let B = (B1,B2) be an (n, ε)-Bloom filter with a steady representation. B is an (n, t, ε)-adversarial resilient Bloom filter (with a steady representation) if for all sufficiently large $\lambda \in N$ and for any probabilistic polynomial-time adversary A we have that the advantage of A in the following challenge is at most ε:

1. Adversarial Resilient: $\Pr[\text{Challenge}_{A,t}(\lambda) = 1] \leq e$,

where the probabilities are taken over the internal randomness of B1 and A and where the random variable ChallengeA,t(λ) is the outcome of the following game:

$\text{Challenge}_{A,t}(\lambda)$:

1. $M \leftarrow B_1(S, 1^{\lambda})$.

2. $x^* \leftarrow A^{B2(M,\cdot)}(1^{\lambda}, S)$ where A performs at most t queries x1, . . . , xt to the query oracle $B_2(M, \cdot)$.

3. If x* /∈ S ∪ {x1, . . . , xt} and $B_2(M, x^*) = 1$ output 1, otherwise output 0.

Test Case : Optimal Margin Classifier for Secure Adaptive Filter

The expert panel are trying to explore whether an efficient privacy preserving optimal margin classifier (e.g. support vector machine) can be applicable for packet classification in communication network and webmail spam filtering. It is an interesting issue whether secure adaptive filter is a private classification problem where SVM can improve the accuracy of classification without false positive or false negative as compared to the use of traditional Bloom or Cuckoo fulter. Another issue is cost of computation and cost of communication. Here, the most important issue is the performance of SVM in terms of classification accuracy and privacy of data. Classification comprises of two subtasks: learning a classifier from training data with class labels and predicting the class labels for unlabeled data using the learned classifier. Data can be stored as feature vectors. In the classification problem of detecting email spam, the training data comprises of emails with labels spam / nospam.

***Support Vector Machine (SVM)* is the most well-known kernelized maximum margin classifier. The learning methodology is the approach of using examples to synthesize programs for computing the desired output from a set of inputs; it generates target decision function in hypothesis space. The learning algorithm selects training data as input and selects a hypothesis from the hypothesis space. There are various methods of learning such as supervised learning from taining examples,**

unsupervised learning, batch learning and online learning. The next issue is generalization - how to assess the quality of an online learning algorithm? Consistent hypothesis performs correct classification of the training data. The ability of a learning machine to correctly classify data not existing in the training set is known as generalization. How to improve generalization : Ockham's Razor suggests that unnecessary complications are not helpful; it may results overfit.

Support Vector Machine (SVM) is a learning system that uses a hypothesis space of linear functions in a high dimensional feature space, trained with a learning algorithm from optimization theory that implements a learning bias derived from statistical learning theory. In case of pattern classification problem, the objective of SVM is to devise a computationally efficient way of learning for finding out an optimal capacity of the pattern classifier to minimize the expected generalization error on a given amount of training data by maximizing the margin between training patterns and class boundary. The basic properties of SVM are that the learning system is suitable for both linear and nonlinear problems, computationally efficient algorithm through modular and dual representation in Kernel induced high dimensional feature space and optimized generalization bounds. Let us discuss about learning in kernel induced feature space.

Target Function – $f(m_1,m_2,r) = C*m_1*m_2/r^2$

$g(x,y,z) = \ln f(m_1,m_2,r) = \ln C + \ln m_1 + \ln m_2 - 2 \ln r = c+x+y-2z$

A linear machine can learn g but not f. A kernel is a function K such that for all x,z ε X ;$K(x,z) = <\varphi(x). \varphi(z)>$ where φ is a mapping from input space X to inner product feature space F.

$<x.z>^2 = (\Sigma^n{}_{i=1}\, x_i\, z_i)^2 = (\Sigma^n{}_{i=1}\, x_i\, z_i)\, (\Sigma^n{}_{j=1}\, x_j\, z_j) = \Sigma^n{}_{i=1}\, \Sigma^n{}_{j=1}\, x_i\, z_i\, x_j\, z_j = \Sigma^{n,n}{}_{i,j=(1,1)}\, (x_i\, x_j)\, (z_j\, z_i) = \varphi(x). \varphi(z)$

Let us consider linear classification problem : given a linearly separable training sample $S = ((x_1, y_1), ..., (x_l , y_l))$, the hyperplane (w,b) realizes the maximal margin hyperplane with geometric margin $\gamma = 1/ \|w\|_2$ by solving the optimization problem Minimize <w.w> Subject to $y_i (<w. x_i> + b) \geq 1$ where i = 1,....,l

In case of SVM, the strategy is to find the maximal margin hyperplane in kernel induced feature space.

In case of linear classification problem, the equation of hyperplane –

$f(x) = <w.x> +b = 0$ or, $f(x) = \sum^l{}_{i=1}\, w_i\, x_i +b = 0$; An input $x = (x_{1,....,}\, x_n)$ belongs to positive class if $f(x) \geq 0$; An input $x = (x_{1,....,}\, x_n)$ belongs to negative class if $f(x) < 0$

Decision function: $h(x) = \mathrm{sgn}\, (f(x)) = \mathrm{sgn}(<w.x> +b)$

In case of linear classification problem, functional margin of an example (x_i, y_i) is $\gamma_i = y_i\, (<w.x_i> + b)$

Geometric margin measures the Euclidean distance between an example and the hyperplane, it is expressed as normalized linear function $(w/ \|w\|, b/ \|w\|)$.

Updation rule of SVM algorithm in Primal Form: if γ_i or $y_i\, (<w.x_i> + b) \leq 0$ then $w_{k+1} \leftarrow w_k + \eta y_i x_i$, $k \leftarrow k+1$ $\gamma_i>0$ indicates correct classification of the training example.

Duality is one of the basic features of Support Vector Machines; SVMs can be modelled as Linear Learning Machines in a dual fashion. In this case, updation rule of the perceptron algorithm is expressed in dual form. The solution i.e. final

hypothesis of weight vector is a linear combination of training points. Each pattern x_i is associated with an embedding strength α_i , which is proportional to the no. of times misclassification of x_i causes updation of the weight.

$w = \sum^{l}_{i=1} \alpha_i y_i x_i$

$f(x) = <w.x> +b = 0$

$= (<\sum^{l}_{i=1} \alpha_i y_i x_i.x> +b)$

$= (\sum^{l}_{i=1} \alpha_i y_i <x_i.x> +b)$

In the dual form, the updation rule and decision function can be expressed in the form of inner product space $<x_i.x>$.

Let us focus on kernel based algorithms; two separate learning functions; learning algorithm in an embedded space; Kernel function performs the embedding; Embed data to a different space; Possibly higher dimension; Linearly separable in the new space. Kernels themselves can be constructed in a modular way. Modularity is one of the important properties of SVM.

Another critical issue is learning in kernel induced feature space : Kernel methods exploit information about the inner products between data items. Kernel function can simplify the computation of separating hyperplane without explicitly carrying out the map in the feature space. The number of operations to compute the inner product space is not proportional to the number of features. Hence, high dimension of feature space does not affect the computation.

Learning In Kernel Induced Feature Space :

Since F is high dimensional, the RHS of this equation is computationally very expensive.

$f(x) = <w.x> +b = (\sum^{l}_{i=1} \alpha_i y_i <x_i.x> +b)$ Eq. of hyperplane in Input Space

$f(x) = <w.\ \phi(x)> +b = (\sum^{l}_{i=1} \alpha_i y_i <\phi(x_i).\ \phi(x)> + b)$ Eq. of hyperplane in Feature Space where ϕ is a mapping from input space to inner product feature space.

$f(x) = \sum^{l}_{i=1} \alpha_i y_i K (x_i.x) + b$ where K = Kernel function

Computation of geometric margin : Geometric margin is the functional margin of a normalized weight vector. In case of linear classifier, the hyperplane function (w,b) does not change if we rescale the hyperplane (mw,mb) where $m \in R^+$ due to inherent degree of freedom. So, to optimize the geometric margin, we can consider functional margin of 1 for two points x^+ and x^-.

$<w.x^+> +b = +1; <w.x^-> +b = -1$

Geometric margin $\gamma = ½(\|w\|_2)\ \ [(<w.x^+> +b) – (<w.x^-> +b)] =1/ \|w\|_2$

SVM Problem Formulation : Given a linearly separable training sample S = ((x_1, y_1), ..., (x_l, y_l)), the hyperplane (w,b) realizes the maximal margin hyperplane with geometric margin $\gamma = 1/ \|w\|_2$ by solving the optimization problem

Minimize <w.w>

Subject to $y_i (<w.\ x_i> + b) \geq 1$ where i = 1,....,l

This is a convex optimization problem minimizing a quadratic function under linear inequality constraints.

Primal Form ---- $L(w, b,\alpha) = 1/2<w.w> - \sum^{l}_{i=1} \alpha_i [y_i (<w.x_i> + b) - 1]$

SVM Problem Formulation

$\partial L(w, b,\alpha)/\partial w = w - \sum^{l}_{i=1} \alpha_i y_i x_i = 0$

$\partial L(w, b,\alpha)/\partial b = \sum^{l}_{i=1} \alpha_i y_i = 0$

$w = \sum^{l}_{i=1} \alpha_i y_i x_i$

Dual Form -----

$L(w, b,\alpha) = 1/2<w.w> - \sum^{l}_{i=1} \alpha_i [y_i (<w.x_i> + b) - 1]$

$\qquad = \sum^{l}_{i=1} \alpha_i - 1/2 \sum^{l}_{i=1} \alpha_i\alpha_j y_i y_j< x_i x_j>$

[Quadratic form]

SVM problem formulation is as follows : Given a linearly separable training sample S = ((x$_1$, y$_1$), ..., (x$_l$, y$_l$)), the hyperplane (w,b) realizes the maximal margin hyperplane with geometric margin $\gamma = 1/ \|w\|_2$ by solving the optimization problem in Dual Form

$$\text{Maximize } \sum^{l}_{i=1} \alpha_i - 1/2 \sum^{l}_{i=1} \alpha_i\alpha_j y_i y_j< x_i x_j>$$

$$\text{Subject to } \sum^{l}_{i=1} \alpha_i y_i = 0$$

$\alpha_i \geq 0$

$w^* = \sum^{l}_{i=1} \alpha^*_i y_i x_i$ = Desired solution

$b^* = ½ [\max_{yi = -1}< w^*.x_i > + \min_{yi = 1}< w^*.x_i >]$

Optimal Hyperplane ---

$f(x,\alpha^*,b^*) = \sum^{l}_{i=1} \alpha^*_i y_i <x_i.x > + b^*$

The advantages of SVM is no local minima due to convexity of the quadratic optimization problem, it is an advantage over neural networks. The open issue is speeding up the training method, choice of appropriate Kernel functions and use of Kernel methods in other algorithms.

3. STRUCTURE

Structure Analytics

Dr. Aziz is analyzing the structure of the systems associated with emerging digital technologies. There are various types of deployment models in cloud computing such as private cloud, public cloud and hybrid cloud. Private cloud is operated solely for a single organization managed internally or by a third party and hosted internally or externally. Public cloud offers a set of services over a network that is open for public use. Hybrid cloud offers the benefits of public and private cloud. In cloud architecture, multiple cloud components communicate with each other over a loose coupling mechanism (e.g. messaging queue). Cloud computing service models are arranged as layers in a stack : Infrastructure-as- a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Database-as-a-Service (DaaS), Datastorage-as-a-Service (dSaaS), Mobile-backend-as-a-Service (MBaaS), serverless computing and Function-as-a-Service (FaaS) [1-20].

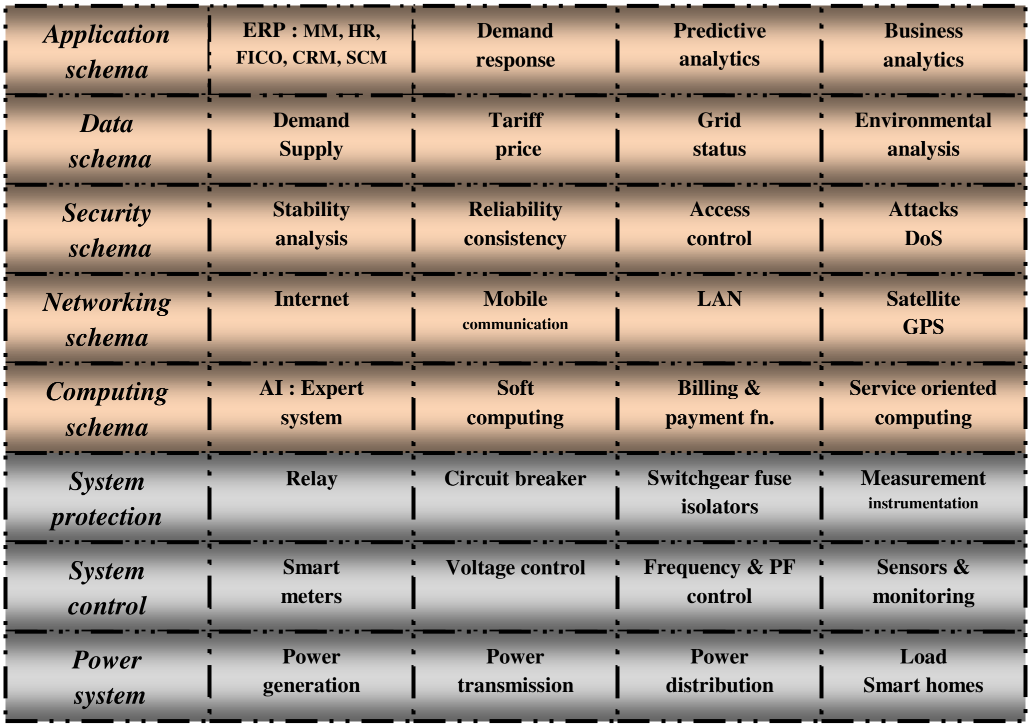
IaaS provides online services of network infrastructure such as physical computing resources, location, data partitioning, scaling, security and backup from data centers. PaaS offers a development environment to application developers through programming languages, libraries, services and various tools. The service consumer does not manage or control the underlying cloud infrastructure (e.g. network, servers, operating systems or data storage) but has control over deployed applications and possibly configuration settings for the application hosting environment. SaaS permits a service consumer to use the software applications of

the service provider running on a cloud infrastructure. The applications are accessible from various client devices through web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure but can access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. MBaaS permits web app and mobile app developers linking their applications to cloud storage and cloud computing services through application programming interfaces (APIs). Serverless computing permits cloud provider fully manageing starting and stopping virtual machines. FaaS is a service hosted remote procedure call that leverages serverless computing to enable the deployment of individual functions in the cloud that run in response to events.

IIoT**: IoT is the network of physical objects embedded with sensors, software and network connectivity that enables the objects to monitor, collect, exchange and analyze data. Industrial Internet of Things (IIoT) is a set of hardware and software components (e.g. smart sensors and actuators) enabled by IoT to support manufacturing and industrial processes. IIoT leverages the power of smart machines and real-time analytics across several industries such as manufacturing (Industry 4.0), logistics, oil, gas, transportation, energy, utilities, mining, metals and aviation. The benefits of IIoT may include better connectivity, scalability, cost savings, improved productivity and better analytics for predictive maintenance.**

Pervasive & wearable computing **: One of the most promising emerging digital technology is health monitoring smart wearable systems (SWS) through advances of micro-electro-mechanical systems, electrical simulation, mechatronics, sensors, actuators, biomedical instrumentation and nanotechnology. SWS is an interesting cost-effective solution which can monitor a patient's health status in real-time and support complex healthcare applications for disease prevention, symptom detection and medical diagnosis. Let us consider the structure of smart wearable system (SWS). The system may have various types of digital and mechatronics components such as sensors, actuators, power supplies, wireless communication units, processing units, algorithms, software, user interfaces and smart fabrics to capture and process data and make intelligent decisions based on the measurement of various parameters of human body such as temperature, blood pressure, heart rate, respiration rate, blood oxygen saturation and ECG. The measured data are sent to a central node (e.g. PDA, medical centre) through wireless communication system. SWS is expected to monitor the state of the health of human agents (e.g. patients, athletes, issue alerts and send feedback to the medical staff in real-time. The healthcare experts and consultants can take rational decisions on patient care accordingly. There are various issues and challenges in telecare, telehealth and telemedicine through new models, prototypes, test beds and industrial products to enhance the performance of healthcare system and minimize the risk of illness, injury, inconvenience and rehabilitation. But, there are various constraints such as high cost, size, weight, energy consumption, complexity of sensor implementation and connectivity, ethics, laws, information security and privacy, freedom, autonomy, reliability, consistency, safety and service issues.**

Edge computing **needs the support of a distributed and open IT architecture having decentralized processing power, mobile computing and IoT technologies. Data is processed by the device itself or by a local computer or server, rather than being transmitted to a data center. Edge structure consists of servers, applications, content distribution network and small clouds at the edge. An edge gateway is a virtual router in either a compact or a full configuration. Edge devices are used by enterprises and service providers through cloud computing and IoT technologies for more intelligence, computing power and advanced services at the network edge. Edge structure uses cloud infrastructure but keeps assets at the edge of the network. A version of the client's apps may run locally to allow ready use without latency, with another versions residing in the regional and central data centers for data warehousing and mining.**



Application schema	ERP : MM, HR, FICO, CRM, SCM	Demand response	Predictive analytics	Business analytics
Data schema	Demand Supply	Tariff price	Grid status	Environmental analysis
Security schema	Stability analysis	Reliability consistency	Access control	Attacks DoS
Networking schema	Internet	Mobile communication	LAN	Satellite GPS
Computing schema	AI : Expert system	Soft computing	Billing & payment fn.	Service oriented computing
System protection	Relay	Circuit breaker	Switchgear fuse isolators	Measurement instrumentation
System control	Smart meters	Voltage control	Frequency & PF control	Sensors & monitoring
Power system	Power generation	Power transmission	Power distribution	Load Smart homes

Figure 10.3 : Information System Structure for Solar Computing

Dr. Aziz is analyzing a smart grid in terms of various system components such as power generation, transmission and distribution system, generators, transformers, transmission lines, loads, switchyards, microgrids comprising of AC/DC sources and loads, renewable energy sources and energy storage system. Figure 10.3 shows the layered structure of a smart power grid having two core layers: (a) physical and (b) information. The physical layer consists of bottom three layers. The first layer connects various components of a power system such as power generation, transmission, distribution and loads. The next layer is system control which consists of smart meters, voltage, frequency and power factor controllers, sensors and

monitoring instruments. Smart meters are able to support exchange of real-time information on demand and supply of electrical power from a smart grid. The meter reading may be communicated to the consumers through SMS and e-mail. The third layer protects the smart grid through various types of relays, circuit breakers, switchgears, fuses and isolators.

The next layer of the smart grid structure is information layer which is associated with computing, networking, security, data and application schema. This layer aggregates information from the physical layer and analyzes data intelligently. The computing schema uses knowledge based expert system and various soft computing tools for automated system control of the smart grid. It is also necessary to compute bills or invoices for the consumers based on consumption of energy; The basic building blocks of networking schema are internet and mobile communication systems. The data schema manages data on demand and supply, tariff and pricing plans. The application schema has various components such as ERP, SCM, CRM, DSS and business analytics; the ERP system may have materials management, finance and cost control, HR and maintenance modules.

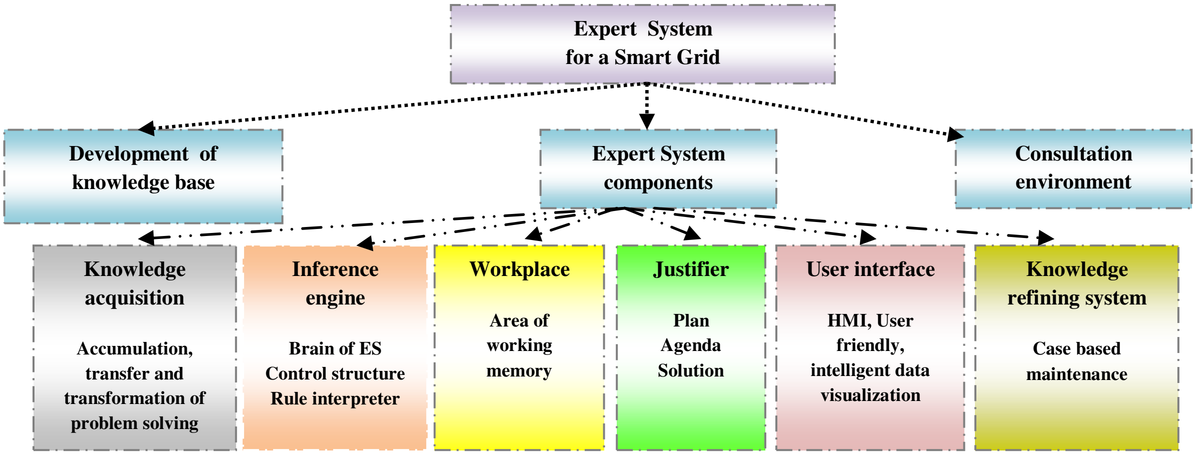

Expert System for a Smart Grid
Development of knowledge base
Expert System components
Consultation environment
Knowledge acquisition
Accumulation, transfer and transformation of problem solving
Inference engine
Brain of ES Control structure Rule interpreter
Workplace
Area of working memory
Justifier
Plan Agenda Solution
User interface
HMI, User friendly, intelligent data visualization
Knowledge refining system
Case based maintenance

Figure 10.4 Expert System for a Smart Grid

The solar computing system should be able to interact with the consumers on various issues such as demand response schemes, current energy sources, information on availability of power, peak load, energy consumption, payments, discounts, variable pricing mechanisms and charging of electrical and hybrid vehicles. The objective of demand response schemes is to accommodate variable supply of renewable energy sources and high frequency monitoring of demand and supply for smart homes, buildings and micro-grids. Solar computing considers the scope of various types of emerging applications such as internet of energy, smart homes and autonomous micro-grids to manage and monitor the use, storage and production of electrical energy though a network of automated modules.

Expert systems are computer based information systems that use expert knowledge to attain high level decisions performance in a specific problem domain [Figure 10.4]. The basic principles of ES include how to determine who experts are, the definition of expertise, how expertise can be transferred from an agent to a computer, how the system works. An expert is an agent who has special knowledge, judgement, experience and methods to give advice and solve problems. The knowledge is basically a set of facts and rules. An ES is expected to recognize and formulate a problem, solve a problem quickly and correctly, explain a solution, learn from experience, restructure knowledge, breaking rules if necessary, determining relevance and degrading gracefully. Expertise is extensive task specific knowledge that use expert process. The level of expertise determines the performance of a decision. Expertise is obtained in various ways ; implicit knowledge is gained from experience; explicit knowledge is gained through supervised learning. Expertise is associated with high degree of intelligence, learning from past success and mistakes, well stored, organized and quickly retrievable knowledge from an expert who has excellent recall of patterns from previous experience. The knowledge is related to a specific problem domain, rules and procedures, heuristics about what to do in a given problem situation, global strategies for solving a problem, meta knowledge (knowledge about knowledge) and facts about problem areas.

Dr. Aziz is presenting the complexity analysis on the structure of IIoT enabled ICS and SCADA technology in terms of various components such as PLC, RTU, field devices, intelligent electrical and electronic devices, workstations, human machine interface, communication gateways, data historians, controllers and software applications; their functions, topology, connectivity and communication protocols. The configuration and scope of an ICS may be simple, medium or highly complex; may be fully or semi-automated. There are various types of ICS like SCADA, process control system (PCS), distributed control system (DCS), safety (SIS), building automation system (BAS), energy management system (EMS) and embedded system (ES).

A Process Control System (PCS) controls an automation process in an industrial plant (e.g. steel, chemical, life-science). SIS monitors an automation process and prevents an unsafe plant operation through a set of sensors and controllers. DCS controls multiple automation processes at a plant (e.g. oil refineries, water treatment plant). BAS monitors and controls a building's infrastructure services such as heating, ventilation, air conditioning, cooling, lighting, elevators, fire protection, energy management etc. through intelligent Internet Protocol (IP). EMS monitors and controls a smart power grid.

SCADA is a type of ICS which collects data and monitors an automated power plant. SCADA control center monitors and manages RTUs and IEDs; the human operators or supervisors use HMI or a supervisory control software to control the power plant by changing set points. A SCADA system may supervise one or more DCSs or PCSs at distant locations, through intelligent communication protocols wherein bandwidth, reliability, latency and jitter are critical success factors. A SCADA system is a process automation system; it is used to gather data from the sensors and the instruments distributed at remote sites and to transmit the data into a central system for controlling or monitoring the basic mechanism. The system controller can view the data collected from the sensors on SCADA host computers located at master site. Automated or operator driven supervisory commands are

transmitted to the control system based on the data received from the remote sensors.

Generally, a SCADA system is composed of five basic components [1]: (i) a sensor network that senses process variables at remote site, (ii) a set of operating instruments connected to the sensors, (iii) a set of local processors that collect data and communicate with programmable logic controllers (PLC), RTU, intelligent electronic devices (IED), transducers, relays and process controllers; (iv) SCADA servers / host computers / master terminal units (MTU) as central point of process control, performance monitoring, data warehousing and data mining and (v) wired / wireless communication channels between local processors and host computers.

Let us do the technical analysis on various components of an industrial control system &/ SCADA. A PLC is a microprocessor controlled electronic device that reads input data from sensors, executes programmed instructions based on input and supervisory control, generate output signals for change of switch settings or actuators. A PLC has CPU, communication interface, input and output modules and power supply and executes various types of programming languages such as ladder diagram, block diagram, structured text, instruction list and sequential function chart. A RTU is a microprocessor controlled electronic device and of two types such as station and field RTUs. Intelligent Electronic Devices (IED) may have one or more processors and can interact with various external entities like digital relays and meters.

A workstation is typically a computer or server running a standard operating system; hosts the programming software for making changes in the logic of the controllers and other applications. HMI is a software application which provides alarms, process status and data trends of an automated processes to a plant supervisor. An HMI can operate on various platforms such as desktop computers, tablets, smart phones or SCADA panel screens. *Data Historian* is a software application for time series analysis of real-time data. *Communication Gateway* enables two devices to communicate with each other. A Front End Processor is a dedicated communications processor. There may be various types of field devices like sensors, transducers and actuators which directly interface with a controller through digital or analog I/O module or industrial protocol (e.g. Modbus). The typical architecture of SCADA supports TCP, IP, UDP and wireless communication protocols as well as Modbus TCP, private radio, cellular or satellite networks [6]. The selection of appropriate communication schema depends on various factors such as data rate, polling frequency, distance, area, budget and future needs. A SCADA system can monitor and control thousands of input / output (I/O) points. This is a complex integrated system: a SCADA network may be integrated with other different types of information and communication systems such as web enabled enterprise applications and business intelligence solutions [3,4]. This architecture provides a real-time, fault-tolerant and intelligent distributed computing platform.

Let us do system audit analysis on digital transformation of ICS / SCADA [Figure 10.5]. In many plants, ICS and SCADA were installed a long time back. It is possible to improve the system performance and productivity of various old plants through system audit grid analysis : divest the dead, old and obsolete technologies (e.g.

electromagnetic relays, PLCs) and invest on emerging technologies (e.g. digital relay protection, sensor networks, Internet communication protocols, self healing system, AI based plant) for digital transformation.

What are the benefits of deploying wireless communication schema in ICS and SCADA? It is a costly strategic option; it requires high capital allocation and technological skill for the replacement of wired networking schema with wireless schema and extensive upgrading efforts. This initiative of digital transformation also requires the replacement of critical electrical and electronic equipments such as digital relays, digital smart meters and sensors which should be fit for operation in wireless environment. It is also important to look into security and privacy of critical data in wireless environment against malicious cyber and physical attacks. It is really challenging to select appropriate wireless technologies for multi-tiered ICS & SCADA architecture. A typical wired ICS infrastructure may be damaged due to natural disaster or act of terrorism. However, there are several benefits of wireless schema in terms of network bandwidth, high speed, reliability, adaptability, availability, safety, scalability, reduced cost of cabling and installation, flexible installation, adhoc ondemand deployment, providing redundancy and efficient integration among different components of plant.

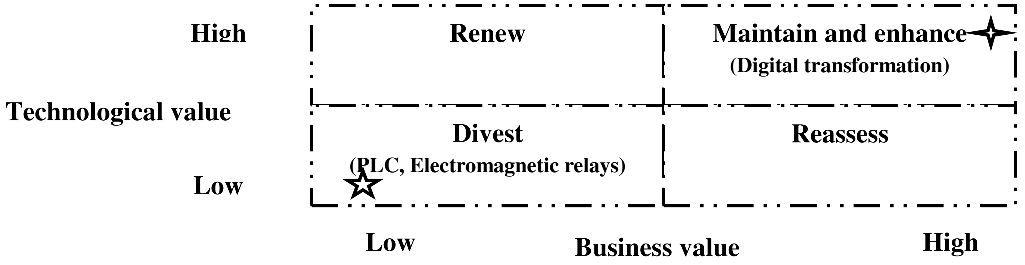


Figure 10.5 : System Audit Grid for IIoT enabled SCADA / ICS

Let us explore the structure of quantum computing model in terms of quantum bits, quantum gates, quantum algorithms and quantum circuit. What are the basic elements of secure multi-party quantum computing model : computing schema, data schema, networking schema and application schema?

***Quantum bits*: A bit is the fundamental building block of classical computation and information. Secure Multi-party Quantum Computation (SMQC) is built upon an analogous concept quantum bit or qubit. Qubit is a mathematical object with specific properties. Qubits are abstract mathematical objects to construct a general theory of SMQC. A bit has two possible states – 0 and 1. Like classical bit, qubit has two possible states |0> and |1> where |> is Diract notation. The difference between bits and qubits is that a qubit can be in a state other than |0> and |1>. It is also possible to form linear combination of states known as superposition. $|\Psi> = \alpha.|0> + \beta.|1>$; where α and β are complex numbers. The state of Qubit is a vector in 2-dimensional complex vector space. The special states |0> and |1>. are known as computational basis states and form a orthogonal basis for vector space. In classical**

computation, a bit is examined whether it is in a state 0 or 1. We can not examine a qubit to determine its quantum state i.e. the values of α and β. We can only acquire much more restricted information about the quantum state. When we measure Qubit, we get either the result 0 with probability α^2 or result 1 with probability β^2. In general, a qubit's state is a unit vector in 2D cvomplex vector space. Another important issue is *multiple qubits* : if there are two bits, there will be four possible states – 00,01,10 and 11. If there are 2 qubits, there will be 4 computational basis states |00>, |01>. |10> and |11>. The state vector describing 2 qubits is |Ψ> = α_{00}.|00> + α_{01}.|01>α_{10}.|10>α_{11}.|11>.

Quantum computation : **A classical computer is built from an electrical circuit containing wires and logic gates. A quantum computer is built from a quantum circuit and elementary quantum gfates to execute secure multi-party quantum computation. Let a system has two states |0> and |1>. Then quantum NOT gate : |Ψ'> = α.|1> + β.|0>.**

Quantum NOT gate , X = [0, 1; 1, 0]; Quantum state α.|0> + β.|1> = [α, β]; X. [α β] = [β, α]

Z ≡ [1 0;0 -1], H = 1 / root 2 [1, 1; 1, -1]

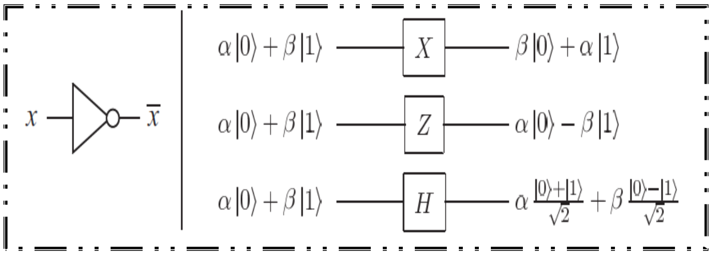

x
$\bar{x}$
$\alpha|0\rangle + \beta|1\rangle$
X
$\beta|0\rangle + \alpha|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$
Z
$\alpha|0\rangle - \beta|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$
H
$\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Figure 10.6 : Qubit logic gates (a)NOT gate, (b) Z gate; (c) H gate

There are various types of quantum gates such as AND, NAND,OR,NOR,XOR, Z gate and H gate; H gate reprents Hadamand operation, a rotation of a space about y axis by 90^0 followed by a rotation of X axis by 180^0.

Quantum circuit **: It is made of quantum gates and wire. Let a circuit swaps the states of two qubits.**

|a,b> → |a, a⊕b>; |a⊕ (a⊕b), a⊕b> = |b, a⊕b>; |b⊕ (a⊕b) ⊕ b> = |b,a>

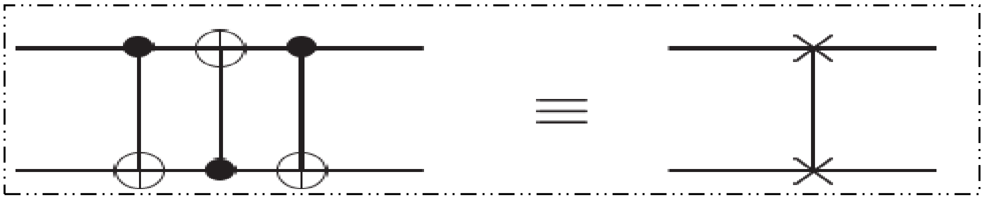


Figure 10.7 : Qubit circuit swapping 2 qubits

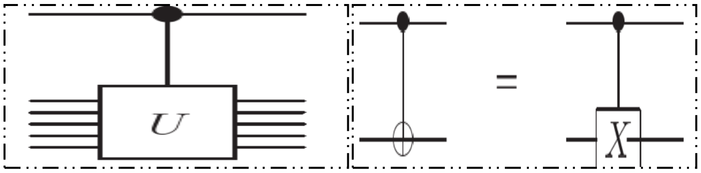


Figure 10.8 : Controlled U gate and NOT gate

Quantum algorithms **: What class of computation can be performed using quantum circuit? How to compute SMQC with computation using classical logic circuits ?**
Toffoli gate **: It has 3 input bits and 3 output bits. It is a reversible gate. Two bits are controlled bits that are unaffected by the action of Toffoli gate. The third bit is a target bit that is flipped if both control bits are set to 1 and otherwise left alone.**
(a, b, c) → (a,b, c⊕a.b) →(a, b, c)
Truuth table of Toffoli gate **:**
Input - [0,0,0;0,0,1;0,1,0;0,1,1;1,0,0;1,0,1;1,1,0;1,1,1];
Output – [0,0,0;0,0,1;0,1,0;0,1,1;1,0,0;1,0,1;1,1,1;1,1,0];
Quantum parallelism **: It is a fundamental feature of many quantum algorithms. It allows quantum computers to evaluate a function f(x) for any different values of x simultaneously.**

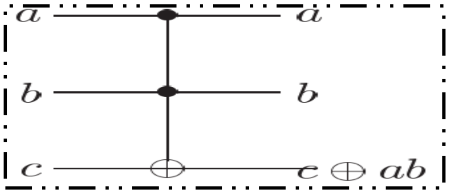


Figure 10.9: Tofolli gate

Structure Analytics

- **Bloom filter**
  - **Adaptive Bloom Filter /**
- **Cuckoo filter**
  - **Adaptive Cuckoo Filter /**
    - **Cuckoo hash table**
- **Parallel pipeline**

Data structure is the basic building block of efficient algorithms. It is used to organize a large amount of data which can be queried efficiently. Randomized data structure assumes that inputs and queries are independent of its internal randomness. For any sequence of inputs, an efficient data structure yields a correct answer with high probability over its iternal randomness. Tere are various types of structure of secure adaptive filter such as Bloom filter, Cuckoo filter, Adative cuckoo filter and parallel d-pipeline.
Bloom filter **: It is a simple space-efficient randomized data structure to represent a set to support membership queries. It allows false positives but the space savings often outweigh this drawback when the probability of an error is controlled. The fundamental principle of the filter is that wherever a list or set is used, and space is at a premium, it is rational to select Bloom filter if the effect of false positives can be mitigated. It exists in an adversarial model if one way function exists. It is used for**

query processing in database and also networking applications. Let, a set S = {x_1, x_2, . . . , x_n} of n elements is described by an array of m bits, initially all set to 0. A Bloom filter uses k independent hash functions h_1, . . . , h_k with range {1, . . . , m}. These hash functions map each item in the universe to a random number uniform over the range {1, . . . ,m}. For each element x ∈ S, the bits $h_i(x)$ are set to 1 for 1 ≤ i ≤ k. A location can be set to 1 multiple times, but only the first change has an effect.

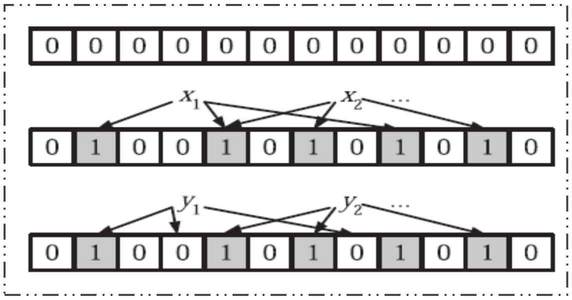


Figure 10.10 : Bloom Filter

Let us check if an item y is in S, we check whether all $h_i(y)$ are set to 1. If not, then clearly y is not a member of S. If all $h_i(y)$ are set to 1, we assume that y is in S, although we are wrong with some probability. Hence, a Bloom filter may yield a false positive, where it suggests that an element x is in S even though it is not. For many applications, false positives may be acceptable as long as their probability is sufficiently small. In figure10.10, a Bloom filter begins as an array of all 0s. Each item in the set x_i is hashed k times, with each hash yielding a bit location; these bits are set to 1. To check if an element y is in the set, hash it k times and check the corresponding bits. The element y_1 cannot be in the set, since a 0 is found at one of the bits. The element y_2 is either in the set or the filter has yielded a false positive.

Cuckoo filter : It is an approximate membership check data structure based on cuckoo hash tables. Instead of storing set elements, it stores fingerprints of the elements using an additional *hash function*. It uses less space but ensures a low false positive probability. Cuckoo hash tables provide an efficient dictionary data structure; it is implemented as a collection of d subtables composed of b buckets each with each bucket having c cells. The hash table uses d hash functions (h_1; h_2;...h_d), where the domain is the universe of possible input elements and the range is [0; b]. The structure supports: look up, insertion and deletion operations as stated in aforesaid secure adaptive filter algorithm.

Adaptive Cuckoo Filter : ACF is a data structure for approximate set membership that extends the concept of cuckoo fillters by reacting to false positives and removing them for future queries. In packet processing application, queries may correspond to flow identifiers; a search for an element is likely to be followed by repeated searches for that element. Removing false positives can significantly lower the false positive rate. ACF uses a *cuckoo hash table* to store fingerprints. ACF is able to significantly reduce the false positive rate; ACF is an approximate membership check structure that can remove false positives selectively without

introducing false negatives. In contrast with the cuckoo fillter, where movements in the cuckoo table can be based solely on the finnger-prints, ACF has original elements available in a slower, larger memory. When inserting a new element, existing elements can be moved. The removal of false positives is almost as simple as a search operation and does not substantially impact the performance of the filter. The structure of ACF is defined in terms of a set of parameters : number of tables used in the Cuckoo hash (d), number of cells per bucket (c), total number of cells over all tables (m), number of buckets per table [b = m/ (d.c)], occupancy or load (l) and number of bits used for fingerprints (a).

4. SECURITY

Security Analytics

Prof. Kamal Kumar, Prof. Simon Watson and Dr. Henry Plank are analyzing the security intelligence of emerging digital technologies. An information system (IS) may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. Emerging digital technologies demand the support of adaptive security architecture so that the associated information systems can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of an emerging digital technology that monitors IS in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, IS should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of an information system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks.

The basic objective of emerging adaptive security architecture and dynamic data protection mechanism is to assess and mitigate the risks of enterprise information system rationally and intelligently. What constitutes an effective strategy of IS security schema? It is debatable whether the proactive approach to IS security is superior to reactive approach. It is possible to recommend an interesting strategy: reactive security may be competitive with proactive security as long as the reactive approach learns from past attacks instead of overreacting to the last attack on the information system. It is not a trivial problem and needs the support of an efficient security protocol from intelligent threat analytics and adaptive security architecture. The following section presents the construction of an adaptive security algorithm to ensure the security of an information system based on proactive and reactive approaches. The basic building blocks of the algorithm are intelligent threat analytics, cryptographic solutions and dynamic data protection. It is basically an attempt of the cross fertilization of algorithmic game theory and cryptography.

It is essential to verify the security intelligence of a smart grid at various levels : L_1, L_2, L_3, L_4 and L_5. At level L_1, the system performance of the grid is verified in terms of reliability, consistency, stability, robustness, safety, liveness and resiliency. Resiliency measures how fast a system can return to the normal operation following a disruption. The other critical factors are deadlock-freeness and synchronization.

The next level is L_2 wherein it is required to audit the access control policy of the grid in terms of authentication, authorization, correct identification, privacy, confidentiality, commitment and trust of the users and the system administrator. At level L_3, the security schema is verified in terms of fairness and correctness (e.g. accuracy of measurement of data in meter reading). At level L_5, it is crucial to assess the risks of various types of malicious attacks on a smart grid such as denial of service (DoS), Sybil and false data injection attack.

At level L_4. it is essential to verify the efficiency of digital relay protection of the transmission lines, generators and motors connected to the power grid such as overcurrent, earth fault, short circuit, voltage and reactive power control and distance protection. Digital relays protect the power system from the adverse effects of a fault which occurs as a random event. The fault current is always greater than the normal load current. If the faulty power system component is not isolated from the grid in time, it may lead to instability. A protection system may consist of CT / PT, CVT, battery, circuit breaker, transducers and protection relays. Overcurrent relays can be used to protect transmission lines, transformers, generators and motors. Reliability and consistency are expected in power system protection. A relay must be dependable and secure; it should operate for specific operating conditions; it should not operate for any other power system disturbance. The responsibility and accountability is defined by a zone of protection. A protection system is responsible for all types of faults occurring within the zone of protection.

Let us present the SWOT analysis on digital power system protection. Smart power grid protection is going through a diffusion of technology from electromagnetic and static relays towards computer enabled digital relays; digital computers have been replacing traditional tools used for short circuit, load flow and stability analysis. Power system protection relays are the next promising scope of computerization based on improved computer hardware, efficient algorithms and programming codes. Digital relays offer the best economic and technical solutions for real-time monitoring and control of power systems today.

Digital relay protection provides several benefits in terms of cost, self-checking reliability, consistency, system integration, adaptive relaying and functional flexibility. The cost of a relay is the main consideration in its acceptability. The cost of digital relays has been declining steadily; the cost of conventional electromagnetic and static relays has been increasing due to change in design, inflation and declining sales and production. A digital relay can be programmed to monitor its hardware and software schema continuously and can detect any malfunctions. It fails in a safe mode and sends a service request alarm to the system center. Digital computers and digital technology have become the basis of measurements, communication, and control of a smart grid. Digital relays can accept digital signals from transducers and fiber optic channels and can be integrated with the control and monitoring system efficiently. Digital computer can be programmed to perform several functions such as measuring and monitoring flows and voltages in transformers and transmission lines, controlling the opening and closing of circuit breakers and switches and providing necessary backup. The relaying function calls for intensive computational activity at no extra cost when a fault occurs on the system. It is an interesting innovation agenda how AI algorithms, heuristics and computing

techniques can be applied in various roles of digital power system protection: (Level A) relaying, switch yard protection, measurements, control, diagnostics, communication with levels B and C; (Level B) man machine interface, data acquisition and storage, sequence of events analyses, coordination, back-up protection, communication with level A and B and (Level C) system control, event analyses, communication with levels A & B, adaptive relaying and system performance analysis.

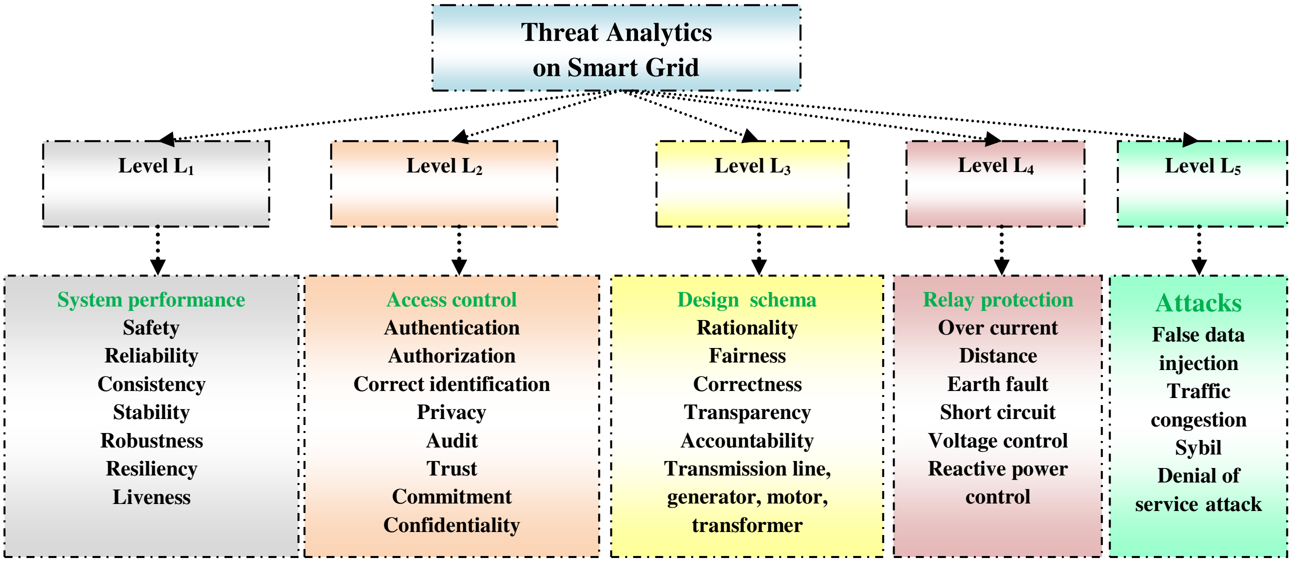


Figure 10.11: Threat Analytics of a Smart Grid

Adaptive security and dynamic data protection : Let us consider the technology associated with adaptive security and dynamic data protection of a smart grid operated through solar computing. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for solar computing. A smart grid demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. Adaptive security is an essential part of solar computing. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

For example, prevention and detection are traditional approaches to the security of a smart grid. In today's digital world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. User Entity Behavior Analytics detect anomalous patterns by comparing with the normal profile and the activities of the users and trigger alarms by sensing single or

multiple attacks on solar computing system. The security must overcome the interorganizational barriers among security, application development and operations teams and be integrated deeply into solar computing architecture.

Dynamic data protection is an effective way to move towards adaptive security architecture. DDP surfaces anomalies and adjusts individualized data security controls proactively in near real-time to protect the critical data of an enterprise. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of organization and networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. This technology is expected to adapt to the needs of solar computing system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of information security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

A system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of a system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. Adaptive security monitors a solar computing system in real time to detect anomalies, malicious traffic and vulnerabilities. If a threat is detected, it is essential to counter the threat in various ways. Preventive capabilities allow the system to create products, processes, and policies that counter-attack malicious attack (e.g. web security) on the solar computing system. The detective capabilities should identify those attacks in time at minimum impact and not detected by preventative capabilities. Retrospective capabilities should perform in-depth analysis of threats not detected by the detective layer to avoid such types of attacks in future. Predictive capabilities provide alerts about external events and anticipates new types of threats.

Abnormal operating conditions and faults may cost a smart grid significantly but may be prevented through intelligent prediction and control mechanism of *knowledge based expert system*. An expert system is expected to monitor, detect and diagnose abnormal conditions of solar power system and provides safeguards against unexpected process conditions. It is possible to model faults and instability in a complex smart grid through expert system which is basically a knowledge based real-time fault diagnostics. The expert system uses the valuable knowledge from the experts, operators and real-time data from various sensors, measuring

instruments and various electrical and electronic devices connected to a smart grid. Soft computing algorithms (e.g. fuzzy logic and ANN) may be used for mining acquired real time data and knowledge discovery from data.

There are two methods of fault diagnosis : model based approach and knowledge based approach. Model based approach adopts quantitative models to estimate states and parameters of system. But, it is almost impossible to obtain a model that exactly matches the process behavior of a smart grid in practice. The mismatch between the behavior of the model and the plant or smart grid may lead to large error signals. Abnormal operation may cause false alarms unless appropriate thresholds are used. It may be impossible to model non-linear systems by analytical equations. These negative aspects demand the support of alternative knowledge based methods in fault diagnosis such as ANN, fuzzy logic and CBR. Knowledge based fault diagnosis is done based on the evaluation of real-time monitored data according to a set of rules which human experts (e.g. operators, engineers, support staff) have learnt from past experience. The knowledge may be input and output process variables, patterns of abnormal process conditions, fault symptoms, operational constraints and performance criteria. Knowledge based approach automates human intelligence for smart grid supervision. Knowledge based approach is suitable for large and complex, nonlinear smart grid. Linear approximation of nonlinear system may result significant errors. The combined approach of knowledge based fault diagnosis with real-time process variables improves the reliability, consistency and efficiency of the system. Knowledge based fault diagnosis has three basic steps: (a) acquire real time process data from sensors and intelligent electrical and electronic devices; the sensed process variables indicate problem of safety and stability of smart solar grid. (b) make inferences or diagnosis based on acquired process data and (c) take actions based on inferences such as raising alarms, informing operators and automated on/off operation of connected equipments for resiliency of the smart grid. Please refer to section 9 which has analyzed the case of a self- healing smart grid through verification of security intelligence at levels L1,L2,L3,L4 and L5.

The next element of the deep analytics is security. The basic building block of security of IIoT enabled ICS and SCADA technology is an intelligent threat analytics. The threats to a plant may be method, target, protocol and identity specific. Insider attacks are more malicious than outsider attacks as the adversaries may have more knowledge about the internal architecture of SCADA & ICS. Method specific threats define how active or passive threats are executed. The method specific threats can be either passive or active. In passive attack, the adversary monitors and analyzes the data captured from SCADA & ICS. In active method, the adversary may send false data to the components of SCADA system.. Target specific threats attack specific component of SCADA network such as PLC, relays and smart meters. The adversaries may try to exploit the vulnerabilities associated with the networking protocols (e.g. DNP3, Modbus).

Please refer to section 9 which outlines security intelligence verification mechanism (SIVM) and also shows its application in three different cases: (a) SCADA for a smart power grid, (b) adaptive industrial control system and (c) defense for border

security surveillance. SIVM is the backbone of the security of IIoT enabled SCADA and ICS technology. Table 4.1 summarizes the major findings of an intelligent threat analytics for the protection of SCADA & ICS in terms of target, risks assessment and mitigation strategies and verification mechanisms. A verification mechanism is expected to provide one or more services by detecting, preventing or recovering from one or more security attacks. We have found that no single verification algorithm can provide adequate security to ICS & SCADA.

Target	*Security Threats on SCADA / ICS*	*Verification mechanisms*	*Risk mitigation strategies*
Networking schema	**Intrusion: sybil, cloning or node replication, wormhole, DoS, node capture**	**Intrusion Verification Mechanism (IVM)**	**Bio-inspired AI: self / non-self classification for negative selection, danger signal detection; identity control**
Networking schema	**Secure communication : Device attestation, false data injection attack, coremelt attack, multicast attack: rushing, blackhole, neighbor, jellyfish**	**Private communication verification mechanism (PCVM)**	**Challenge response protocol, bad data measurement, SCADA network traffic congestion analysis; Key management protocol to preserve group, forward and backward privacy.**
Cyber application schema	**Web service security**	**Web security verification mechanism (WSVM)**	**Trusted service oriented computing**
Computing and application schema	**Biometric access control**	**Access Control Verification Mechanism (ACVM)**	**Biometric enrollment and recognition; credential based access control**
Data schema	**Privacy : inference control**	**Privacy Verification Mechanism (PVM)**	**Statistical disclosure control preserving confidentiality and privacy: randomization, suppression, generalization, sampling, summarization, aggregation.**

Table 10.1: Threat Analytics

An intelligent threat analytics should perform various type of vulnerabilities analysis as follows :
***Vulnerability analysis 1*: Domain (configuration, design specification, implememtation) vs. weakness (account mgmt, poor coding practice, poor authentication, interface programmimg, malfunctioning devices, poor logging, inefficient monitoring);**
***Vulnerability analysis 2* : Risk elements (purpose of attacks [information capture, sabotage], lateral movement [automatic], location command and control server [Insider and outsider attack], initial attack vector [Automatic]) vs. types of attacks (e.g. capture information from target through industrial espionage, identity theft, IP theft, spearphishing, drive-by-download attack);**
***Vulnerability analysis 3* : Classification of vulnerabilities (buffer outflow, forced browsing, code injection, access control, input validation, resource exhaustion, authentication attack, path traversal, resource allocation, weak password, DLL**

hijacking, SQL injection, cryptographic failure, CSRF, weak encryption) vs. history of occurence;
Vulnerability analysis 4 **: metrics (physical, information, cognitive, social) vs. risk mitigation practice (plan, absorb, recover, adapt);**
It is essential to define an optimal set of security metrics in terms of risk and resilience. The metrics are the measurable properties of ICS that quantify the degree to which objectives have been achieved and provide vital information of system performance. Security metrics are associated with critical business functions such as incident, vulnerability, patch, configuration, security and change management. The metrics should be linked to a strategy, can be quantified, comprehensive, and measurable and indicates the right behavior of a system. Relevant Metrics are directly linked to decision making goals, objectives and relevant attributes of a system.

Adaptive security and dynamic data protection

The expert panel are interaction on the technology associated with adaptive security and dynamic data protection of ISI analytics. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for SCADA & ICS which demands continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. ***Adaptive security*** **is an essential part of ISI analytics. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.**
For example, prevention and detection are traditional approaches to the security of SCADA & ICS. In today's digital world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. User Entity Behavior Analytics detect anomalous patterns by comparing with the normal profile and the activities of the users and trigger alarms by sensing single or multiple attacks on SCADA & ICS. The security must overcome the inter-organizational barriers among security, application development and operations teams and be integrated deeply into ISI analytics architecture.
Dynamic data protection **is an effective way to move towards adaptive security architecture. DDP surfaces anomalies and adjusts individualized data security controls proactively in near real-time to protect the critical data of an enterprise. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of organization and networking schema: real time monitoring of events, users and network traffic, autonomous and dynamic resolutions, prioritization and filtering of security breaches, reduction of attack surface and impact or damage of a threat and reduction of resolution time. This technology is expected to adapt to the needs of ISI**

analytics irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of information security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of security architecture.

A system may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An emerging technology demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of a technology that monitors the network or grid associated with a system in real-time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events of a system to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. Adaptive security feature of ISI analytics monitors SCADA & ICS in real-time to detect anomalies, malicious traffic and vulnerabilities. If a threat is detected, it is essential to counter the threat in various ways. Preventative capabilities allow enterprises to create products, processes, and policies that counter-attack malicious attack (e.g. web security) on SCADA &/ ICS. The detective capabilities should identify those attacks in time at minimum impact and not detected by preventative capabilities. Retrospective capabilities should perform in-depth analysis of threats not detected by the detective layer to avoid such types of attacks in future. Predictive capabilities provide alerts about external events and anticipates new types of threats.

Adaptive Security Algorithm [ASA]

***Agents*: Defender (e.g. system administrator), Attacker (e.g. malicious agent or adversary);**

***System* : Enterprise information system;**

***Objectives*: optimize enterprise IS security investment;**

***Constraints*: budget, resources, time;**

***Input*: Enterprise information system performance parameters and architecture;**

***Strategic moves*:**

- **Adaptive security**
- **Dynamic data protection**
- **Self-healing mechanism**
- **Crash proof code**
- **Real-time fault diagnostics**
- **Adoption of hybrid strategy i.e. an optimal mix of proactive and reactive approaches.**

***Revelation principle*: The agents preserve privacy of strategic data;**

- **Defender : The defender does not disclose the proactive and reactive approach of information security to the adversaries.**
- **Attacker : The adversaries preserve the privacy of the plan of malicious attack, information of targets and weak links.**

***Security intelligence verification*:**

- ***Proactive approach*:**
  - ***Threat modeling***
    - **Call threat analytics function (f_a);**
    - **Estimate probability (*p*) of occurrence along two dimensions : Low [L] and High [H];**
    - **Estimate impact of risk i.e. sunk cost (c) along two dimensions : [L,H];**
    - **Map threats into a set of risk profiles or classes : LL, LH,HL and HH;**
    - **Estimate security requirements in terms of demand plan (P_d);**
    - **Develop risk mitigation plan (P_m) : accept / transfer / remove / mitigate risks.**
  - **Identify targets : computing, data, networking and application schema;**
  - **Verify security intelligence of information system in real-time.**
    - ***Data schema* :**
      - **Dynamic data protection :**
        - **check data integrity;**
        - **assess the risks of false data injection and shilling attacks by the intruders;**
        - **verify access control efficiency in terms of authentication, authorization, correct identification, privacy, audit, confidentiality and nonrepudiation;**
    - ***Computing schema*: verify fairness, correctness, accountability, transparency, rationality, trust and commitment in multi-party computation;**
    - ***Networking schema* :**
      - **Verify system performance in terms of reliability, consistency, stability, liveness, deadlock-freeness, reachability, safety, resiliency;**
      - **assess the risks of intrusion, denial of service (DoS), coremelt, Sybil, node replication and wormhole attacks;**
    - ***Application schema***
      - **do penetration testing;**
      - **audit user acceptance, system performance and quality of application integration.**
- ***Reactive approach*:**
  - **adopt sense-and-respond strategy.**
  - **assess risks of single or multiple attacks on the information system; analyze performance, sensitivity, trends, exception and alerts.**
    - **what is corrupted or compromised?**
    - **time series analysis : what occurred? what is occuring? what will occur?**

    - **insights : how and why did it occur? do cause-effect analysis.**
    - **recommend : what is the next best action?**
    - **predict: what is the best or worst that can happen?**
  - **Adjust P_d and P_m.**

***Payment function*:**

- **Estimate aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements.**
- **Trade-off proactive vs. reactive security: assign weights to each risk profile.**
- **Do portfolio rationalization of the security schema.**
- **Select dominant strategy of IS investment from the options of process re-engineering, transformational, renewal, experiment and reinforcement on the weakest link.**

***Output*: Optimal security investment plan**

Real-time Fault Diagnostics

An intelligent adaptively secure system for monitoring, supervisory control, and diagnosis of complex operations of a smart plant may adopt data driven or analytical or knowledge based approach and is expected to have following capabilities [45-51] : (a) coordinate various tasks of process control such as monitoring, diagnosis and supervisory control; (b) integrate the solution approaches of data driven, analytical and knowledge based intelligent systems; (c) the ability to coordinate different schemes of knowledge representations such as rules, frames, models and cases; (d) maintain a global database and global management of process knowledge; (e) maintain a hierarchical structure of data models on controllers, actuators, sensors, logical constraints, process models, faults and processes at various abstraction levels and (f) the ability to adapt to a changing environment of plant operation.

Abnormal operating conditions and faults may cost a plant significantly but may be prevented through intelligent prediction and control mechanism of knowledge based expert system. An expert system is expected to monitor, detect and diagnose abnormal conditions of a plant and provides safeguards against unexpected process conditions. It is possible to model faults and instability in a complex plant through expert system which is basically a knowledge based real-time fault diagnostics. The expert system uses the valuable knowledge from the experts, operators and real-time data from various sensors, measuring instruments and various electrical and electronic devices connected to a plant. Soft computing algorithms (e.g. fuzzy logic and ANN) may be used for mining acquired real time data, inferencing and knowledge discovery from data.

There are two methods of fault diagnosis : *model based approach* and *knowledge based approach*. Model based approach adopts quantitative models to estimate to estimate states and parameters of system. But, it is almost impossible to obtain a model that exactly matches the process behavior of a plant in practice. The mismatch between the behavior of the model and the plant may lead to large error

signals. Abnormal operation may cause false alarms unless appropriate thresholds are used. It may be impossible to model nonlinear systems by analytical equations. These negative aspects demand the support of alternative knowledge based methods in fault diagnosis such as ANN, fuzzy logic and CBR. Knowledge based fault diagnosis is done based on the monitoring and evaluation of real-time data according to a set of rules which human experts (e.g. operators, engineers, support staff) have learnt from past experience. The knowledge may be input and output process variables, patterns of abnormal process conditions, fault symptoms, operational constraints and performance criteria. Knowledge based approach automates human intelligence for plant supervision; it is suitable for large and complex nonlinear plant. Linear approximation of nonlinear system may result significant errors. The combined approach of knowledge based fault diagnosis with real-time process variables improves the reliability, consistency and efficiency of the system. Knowledge based fault diagnosis has three basic steps [Appendix]: (a) acquire real-time process data from sensors and intelligent devices; the sensed process variables indicate problem of safety and stability of the plant; (b) make inferences or diagnosis based on acquired process data; (c) take actions based on inferences such as raising alarms, informing operators and automated on/off operation of connected equipments for resiliency of the plant. Please refer to the case study of Industrial Control System in section 9.2 wherein the concept of RTFD is appropriately applicable.

Analysis of Adaptive Security Algorithm (ASA)

Recently, there is a trend of cross fertilization between two disciplines: game theory and cryptography. Cryptography focuses on secure multi-party computation preserving privacy, fairness and correctness against the threats of malicious agents. Game theory tries to understand the behavior of rational agents with well defined goals in a given situation and designs the rules of interaction. There are differences between the two disciplines based on specific issues such as players, solution drives, incentives, privacy, trust, early stopping, deviation and collusion. Cryptography assumes honest or malicious players; game theory assumes rational players; the solution drivers are secure protocol and equilibrium respectively. Both disciplines study collaborative interactions among the agents with conflicting interests. It is possible to solve traditional game theoretic problems and design of efficient mechanisms using the concept of cryptographic solutions and secure multi-party computation. It is also an interesting research agenda to explore new cryptographic concerns using game theoretic concepts such as secure and fair computation and rational secret sharing. Traditionally, cryptographic solutions are focused on the privacy, fairness and correctness to ensure information security. The domain needs a broad outlook for improved efficiency in new applications.

ASA is associated with the problem of information security investment decisions based on the concept of computer science, economics, management science and related disciplines. It is a complex decision making problem. The existing woks attempt to derive and compare optimal investment strategy exploring the delicate balance between proactive and reactive approaches. The current work is an attempt

to extend the existing research. It presents the construction of a deep learning based algorithmic mechanism to ensure the security of an information system based on proactive and reactive approaches. The basic building blocks of the mechanism are threat analytics, cryptographic solutions and adaptive secure multiparty computation.

ASA is associated with a security game. Game theory is concerned with a complex decision making process in which two or more players interact. Each of these players tries to optimize its own objective function. A game can be classified as cooperative game or a non-cooperative game. In a cooperative game, the players make agreements in order to minimize their common cost or to maximize their common payments. This is not possible in a non-cooperative game. A cooperative game is a game where a group of players enforce a cooperative behavior. The game is defined by (N,u) where N denotes a group of agents and u is a real valued characteristic function. The ASA is defined by various types of elements: a group of agents or players, model, actions, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payments, a strategy profile, a dominant strategy which maximizes the utility of an agent for all possible strategies of other agents involved in the mechanism, security intelligence and revelation principle. There are two agents in the security game: a defender (D) and the attacker (A). Each agent adopts and executes a or a set of strategies. A pure strategy is a deterministic policy for a single move game. For many games, an agent can do better with a mixed strategy. The best strategy may depend on the knowledge of the defender about prospective attacks and the sunk costs incurred when upgrading information security schema reactively. The payment function of the mechanism estimates an optimal investment plan for the security of information system. One of the most critical issues of ASA is revelation principle and verification of security intelligence of the information system schema. The agents preserve the privacy of strategic data. The defender does not disclose the proactive and reactive approach of information security to the adversaries. The adversaries preserve the privacy of the plan of malicious attack. The basic building block of ASA is adaptive security and DDP.

Let us explain the objectives of adaptive security architecture in depth. New threats are getting originated as an outcome of digital technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for the emerging technologies. The systems demand continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach.

For example, prevention and detection are traditional approaches to the security of an information system. In today's world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security but should adopt cloud based solutions and open application programming interfaces also. Advanced

analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture.

Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjusts individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of the system and complexity of networking schema: real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging digital technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

Adaptability is about responding to change effectively and decisively through reactive approach: the ability to identify the change in search space for the adversaries, understanding the probable impacts of the hit by the adversaries, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time without any hesitation. The defender tries to define the requirements of the security schema of an information system in terms of aspiration point, reservation point and adjustment of various preferential thresholds (e.g. indifference, strong preference, weak preference, veto) and preferred solutions. The value of the objective function which is desirable or satisfactory to the decision maker or defender is defined as aspiration point. The value of the objective function that the defender wants to avoid is reservation point. The defender can use various preference thresholds in order to compare alternatives and to define outranking relations. There is an interval of preference wherein it is not possible for the defender to distinguish between different alternatives and this is defined as indifference threshold. Strict preference threshold is defined as minimal increase or decrease of any objective that makes the new alternative strictly preferred with respect to this objective. There exists an intermediate region between indifference and strict preference threshold where the defender may hesitate to compare alternatives. It is defined as weak preference threshold. Veto threshold indicates what is the minimal increase or decrease of any objective that makes the new alternative unacceptable regardless of the value of other objectives.

The adaptive security algorithm evaluates the security intelligence of an information system based on proactive and reactive approaches. Real-time security management involves high cost of computation and communication. The vulnerability of the system to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The defender must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in the operation of the system? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. For example, the map has four quadrants in a two dimensional space; the vertical axis represents the probability of disruptive event and the horizontal axis represents the magnitude of the consequences. The system may face a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the system? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in the vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do real-time system monitoring.

The computational cost of adaptive security algorithm depends on the complexity of threat analytics function (f_a) and payment function (f_p) in terms of investment allocation heuristics.

The cost of computation is a function of the complexity of threat analytics. The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the system: agents, communication schema, data schema, application schema, computing schema and protocol? what occurred? what is occuring? what will occur? assess probability of occurrence (*p*) and impact or sunk cost (c). The analysis on insights may be as follows : how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen? The threat analytics also evaluates the vulnerability of the information system to a disruptive event in terms of likelihood of a disruption and its potential severity. The computational burden is also associated with the identification of a set of feasible risk metrics for each type of threat on the information system, assessment of the probability of each risk metric, computation of severity or sunk cost of each risk metric and plotting each risk metric in the vulnerability map.

Another major computational burden of ASA is the complexity of verification or model checking algorithms. The verification system requires both automated and semi-automated verification options. The verification system calls threat analytics

and a set of model checking algorithms for various phases: exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of the system under consideration. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

The cost of computation also depends on the complexity of payment function. The payment function estimates aspiration point, reservation point, strong, weak, indifference and veto thresholds in the security requirements; makes trade-off proactive vs. reactive security: assign weights to each threat; exercises portfolio rationalization of the security schema and allocates fund based on the selection of invest options. There are various objectives of investment of information security schema such as process re-engineering, transformational, renewal, experiment and reinforcement on the weakest link. The payment function selects appropriate heuristics of fund allocation such as selective based on ranks, linear and proportional allocation. When the budget of the defender is more than the total projected demand, the agent would like to satisfy all the portfolios of IS security schema using the resource allocation function. However, when the budget is less than total demand, the agent should find the investment plan based on various types of allocation heuristics, objectives and constraints .

Linear allocation is an equal sharing of the pain or shortage of capacity among various components of IS security schema. The threat T_i is allocated fund $q_i = d_i - (1/n) \max (0, \sum_{i=1}^{n} d^*_i - C)$ where n is the number of threats and C is the budget capacity of the defender. In case of *proportional allocation*, the threat T_i is allocated fund $q_i = \min \{d^*_i, C.d^*_i/(\sum_{i=1}^{n} d^*_i)\}$. Reactive approach may consider reinforcement learning strategy and allocates more budget to easier-to-defend edges of the attack graph. When new edges are revealed, the budget is reallocated uniformly from the already revealed edges to the newly revealed edges. Myopic bug chasing is most likely an ineffective reactive approach. But, the strategy of gradually reinforcing attacked edges by shifting budget from unattacked edges of the attack graph may be cost effective. Another fund allocation strategy is *selective allocation* based on the computation of the rank of the threats which is computed based on probability of occurrence (*p*) and impact or sunk cost (c).

The security intelligence of ASA is associated with the computing, data, application and networking schema of an information system and is verified through the properties of adaptive secure multi-party computation.

ASA evaluates the security of an enterprise information system in breadth and depth from the perspective of collective intelligence. The targets of the defender are computing, data, networking and application schema of an information system. It is basically a holistic approach which is focused on both proactive and reactive security. ***Let us first consider proactive approach*****. The verification algorithms check fairness, correctness, accountability, transparency, rationality, trust and commitment of the computing schema. It is essential to verify authentication, authorization, correct identification, privacy and audit of data schema. The health of networking schema is verified in terms of safety, reliability, consistency, liveness, deadlock-freeness, reachability and resiliency. The security of application schema is evaluated through penetration testing in terms of user acceptance, system performance and quality of application integration. In case of machine learning with adversarial setting, the ASA also audits the security of data schema and monitors the risk of false data injection attack, noise, missing data and incomplete features and assesses the risk of Sybil attack. The security of application schema is verified in terms of flaws in training and testing strategy (no. of training and testing samples, learning rate), the efficiency of data mining algorithms and knowledge extraction procedure through penetration testing. Penetration testing searches for potential vulnerabilities and it can be modeled to reduce uncertainty in a security game. It is an information gathering option prior to investing into protection against a threat.**

Next let us consider ***reactive approach*** **which adopts sense-and-respond strategy. The basic objective of adaptive secure multi-party computation is to identify the hit of adversaries on computing schema that may choose the corrupted parties during the course of computation. The verification algorithms check the scope of information leakage or violation of privacy in various steps of secure multi-party computation algorithm : adding random noise to data, splitting a message into multiple parts randomly and sending each part to a decision making agent through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly.** ***Adaptability*** **is basically responding to change(s) effectively and decisively: the ability to identify the occurrence of uncommon threats which are not considered in proactive approach; change in system performance, understanding the probable cost of malicious attacks, rapid quantification what is under its control to compensate, identification what modifications to the environment are necessary and adoption of risk mitigation measures in time. The defender adjusts the requirements of the security schema of an information system adaptively in terms of aspiration and reservation point and various preferential thresholds. Adaptive secure multi-party computation identifies what is corrupted or compromised; what has occurred or what is occurring; performs cause-effect analysis for more transparency and insights; decides what the next best action is and also predicts what is the best or worst that can happen.**

ASA shows the importance of an efficient algorithmic mechanism for proper evaluation of the security schema of an information system. It is basically a hybrid approach which recognizes the role of both proactive and reactive approaches in making decisions on investment of IS security schema rationally. The reactive approach may outperform proactive one against the threats that never occur actually. Sometimes, reactive approach may be cost effective as compared to proactive approach. The basic building blocks of the ASA are threat analytics, cryptographic solutions and adaptive security architecture. The threat analytics monitor the system performance based on time series data, detects and analyzes different types of vulnerabilities on enterprise information system. This work finds a set of interesting research agenda for future work: (a) explore new cryptographic concerns using game theoretic concepts and intelligent reasoning; (b) how to design an intelligent threat analytics; (c) how to design automated verification algorithms; (d) how to rationalize adaptive secure multi-party computation protocols and (e) how to quantify and code miscellaneous security intelligence parameters?

Case Analysis **: This section has analyzed three test cases to develop Security Intelligence Verification Mechanism [SIVM] for IIoT enabled SCADA and ICS technology : (a) SCADA for a smart power grid, (b) industrial control system and (c) defense - border security surveillance The basic building blocks of SIVM are a set of security protocols: intrusion verification, private communication, web security verification, biometric access control verification and privacy verification. SIVM is useful to analyze the security element of the deep analytics.**

Test Case 1 : SCADA for a Smart Power Grid

Security Intelligence Verification Mechanism [SIVM$_{PG}$]
System: Intelligent System [Knowledge based system (KBS), DSS/ GDSS, BI]
Input : Sensors data;
Move : Call deep analytics → assess threats on 7-'S' elements;

- ♦ **Scope : SCADA for smart power grid,**
- ♦ **System : Information system having computing, networking, data, application and security schema;**
- ♦ **Structure : Sensors, central server, connecting link or communication channel;**
- ♦ **Strategy :**
    - **Governance :**
        - **proactive approach**
        - **reactive approach**
    - **Automated system verification and model checking**
    - **Goal setting : call deep threat analytics**
    - **Shared vision**
    - **Intelligent Communication protocol for collaborative and collective intelligence**
- ♦ **Security at multiple levels (L1, L2,L3,L4 and L5)**

- **Staff: System administration, technical and maintenance staff, operation team, management consultants;**
- **Skill : technical, management;**
- **Style : Adaptive, resilient leadership style, system coordination, intelligent coordination;**
- **Support: Preventive and breakdown maintenance;**

Revelation principle: Audit privacy and confidentiality of critical data based on information disclosure policy.

Payment function: Audit business intelligence of contracts with the service providers.

Verification algorithms [refer section 9.4]:

1. Call threat analytics.

2. Do *automated verification* of the security intelligence of data, computing, application, networking and security schema at levels 1,2,3,4 and 5.

3. Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities.

Level 1 (*data schema*):

- **Flaws in access control: Authentication, Authorization, Correct identification, Privacy, Audit, Confidentiality, Integrity, Non-repudiation, locking of passwords, false data injection attack;**
- **Intrusion detection;**
- **Data warehousing, data mining, data visualization and performance measurement strategy;**

Level 2 (*computing schema*):

- **Correctness of computation, system configuration and mechanism**
  - **KBS :**
    - **knowledge base, inference engine, user interface, knowledge acquisition and refining subsystem, justifier, workplace;**
    - **case based reasoning through case base maintenance, case retrieval, case adaptation and learning;**
  - **DSS/GDSS :**
    - **Intelligence in search of right conditions;**
    - **Design of possible alternatives;**
    - **Choice of appropriate action or solution;**
    - **Implementation in problem solving or exploiting opportunities;**
    - **Structured / semi-structured / unstructured decision making for operational control / managerial control / strategic planning;**
  - **BIS**
    - **Detection of incomplete, imprecise, noisy or missing data**
    - **Inefficient data mining algorithms with flaws in training and testing strategy**
    - **Flaws in knowledge discovery from data (KDD)**

- **Fairness in resource allocation;**
- **Transparency of process, procedure and mechanism;**
- **Accountability of role in system administration, operation and maintenance;**

Level 3 (application schema):

- **Poor system performance : Denial of Service (DoS) attack, reliability, consistency, resiliency, stability, robustness, liveness, deadlock freeness, lack of synchronization, human error in keying of mobile devices or remote operation;**
- **flaws in web application design : logic attack, cross site scripting, injection flaws, malicious file injection, insecure direct object reference, cross site request forgery, information leakage and improper error handling, broken authentication, session hijack, insecure cryptographic storage, insecure web communication, failure to restrict URL access, flaws in application integration;**

Level 4 (*networking schema*): Identify types of malicious attack : internal and external; Cyber attacks, Rubber hose attack, Sybil attack, Node replication attack, Wormhole attack, Coremelt attack, Forward, Blackhole, Neighbor, Jellyfish, Crypto jacking on mobile devices;

Level 5 (security schema):

- **Assess the risk of multi-party corruption (e.g. sender, receiver, data, communication channel, mechanism and protocol);**
- **Business intelligence of payment function**

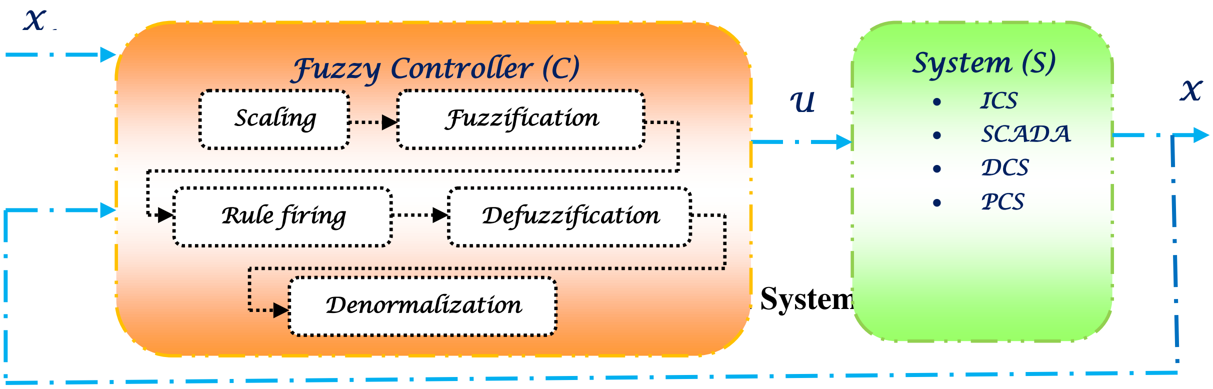
Risk mitigation:

- **Proactive approach**
  - **Call predictive analytics; analyze probability of occurrence vs. impact;**
  - **Call challenge response protocol;**
  - **Preventive maintenance, Technology upgradation, System isolation**
- **Reactive approach**
- **Sense-and-response against bad luck**
  - **Natural disaster : Heavy rainfall, snowfall, storm, cyclone, flood, earthquake;**
  - **Industrial / HR unrest / Political strike**
  - **Accidents**
  - **Terrorism**

3. Adjust device settings automatically.

Output: SCADA performance scorecard; security intelligence.

Test Case 2: Industrial Control System



Security Intelligence Verification Mechanism [SIVM$_{ICS}$]
System: **Industrial Control System;**
Input **: Sensors data;**
Move **: Call deep analytics --> assess threats on 7-'S' elements;**

- **Scope : Supervisory, adaptive, fuzzy control of industrial plant**
  - **Linear model**
  - **Nonlinear model**
- **System : Computing, Networking / Communication, Data, Application and security schema;**
- **Structure : Sensors, central server, connecting link, system, fuzzy controller;**
- **Strategy :**
  - **Governance : proactive and reactive approach, intelligent secure communication protocol, shared vision, goal setting**
  - **Automated system verification and model checking**
- **Security-sensitivity at multiple levels**
- **Staff: System administration, technical and maintenance staff, operation team, management consultants;**
- **Skill : technical, management,**
- **Style : Adaptive, resilient leadership style, system coordination, intelligent coordination;**
- **Support : Preventive maintenance, breakdown maintenance.**

Revelation principle: **Audit privacy and confidentiality of critical data based on information disclosure policy.**
Payment function: **Audit business intelligence of contracts with the service providers.**
Verification algorithms **[refer section 9.4]:**

1. **Call threat analytics.**
2. **Do *automated verification* of the security intelligence of data, computing, application,**

networking and security schema at levels 1,2,3,4 and 5.

3. Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities.

Level 1 (*data schema*): Authentication, Authorization, Correct identification, Privacy, Audit, Confidentiality, Integrity, Non-repudiation, locking of passwords, false data injection attack, intrusion detection through access control;

Level 2 (*computing schema*):

- **Correctness of computation [Reference : Figure 10.2]**
    - **Input scaling i.e. normalization /* For a MISO, x_1, x_2,…,x_n : controller inputs in IF part of fuzzy rules; u_1,u_2.,,,,u_m : controller outputs in the THEN part of fuzzy rules ; Input scaling $E_n = N_e.e$; $E = (e_1,e_2,\ldots e_n)^T$; $E_i = x_i-x_d$; N_e = normalization of factors */**
    - **Fuzzification of controller input variables /* During fuzzification, a crisp controller input x* is assigned a degree of membership to the fuzzy region from IF part of a fuzzy rule*/**

      $E^* = e_1^*$, e_2^*,…e_n^*; e^* : a normalized crisp controller input. $LE^j = LE^j_{11},\ldots,LE^j_n)^T$

      LE^j_n : Fuzzy values taken by the controller inputs
    - **Inference i.e. rule firing /* For a MISO FC, ith fuzzy rule - R^j_c: IF e = LE^j THEN u = LU^j*/**
    - **Defuzzification of controller output variables /* Obtain a scalar value u from membership function CU(u) where U : defuzzified controller output */**
    - **Output scaling i.e. denormalization : $U_N = N_u.u$; /* The defuzzified normalized controller output U_N is denormalized with the help of an off-line predetermined scalar denormalization factor N_u^{-1} */**
- **Fairness in system performance,**
- **Transparency of process / procedure / mechanism.,**
- **Accountability in system administration, operation and maintenance;**

Level 3 (*application schema*):

- **Stability in system performance, robustness, accuracy and speed**
- **Reliability, Consistency, Resiliency, Liveness, Denial of Service (DoS) attack, Deadlock freeness, Lack of synchronization,**
- **Human error in keying of mobile devices or remote operation;**
- **Flaws in application integration;**

Level 4 (*networking schema*): Identify types of attack : internal and external; Cyber attacks, Rubber hose attack, Sybil attack, Node replication attack, Wormhole attack, Coremelt attack, Forward, Blackhole, Neighbor, Jellyfish, Crypto jacking on mobile devices;

Level 5 (security schema) : multi-party corruption [e.g. sender, receiver, data, communication channel, business intelligence in terms of payment function, mechanism, protocol, process, procedure];.

***Risk mitigation*:**

- ***Proactive approach***
    - **Call predictive analytics; analyze probability of occurrence vs. impact ;**
    - **Call challenge response protocol;**
    - **Preventive maintenance, technology upgradation, system isolation;**

- *Reactive approach*
- **Sense-and-respond against bad luck such as natural disaster, accidents and terrorism**

4. Adjust device settings automatically.

Output: SCADA performance scorecard; security intelligence.

Test Case 3 : Defense – Border Security Surveillance

This is a great challenge to the SCADA system administrator, power system planners, analysts, researchers and operators to sustain security and safety of a smart, intelligent energy grid. The proposed verification mechanisms and resilient SCADA are also applicable in sensor networks for defense application, automated continuous production plants, refineries, oil and gas pipelines. For instance, the defense security system of a country I tries to monitor the activities and the movement of the security force, tanks, war ships and weapons manufacturing plant of a neighboring country C by deploying a SCADA network [Figure 7.5]. A base station is built at a strategic location to control the SCADA network; the sensors relay critical data to the base station. The adversary i.e. the defense security system of country C may be able to launch different types of attacks such as sybil attack, physical destruction of sensor nodes, resource consumption attack to deplete the limited energy of the sensors and the attack on routing and data link protocols associated with the defense information and communication system of country I.

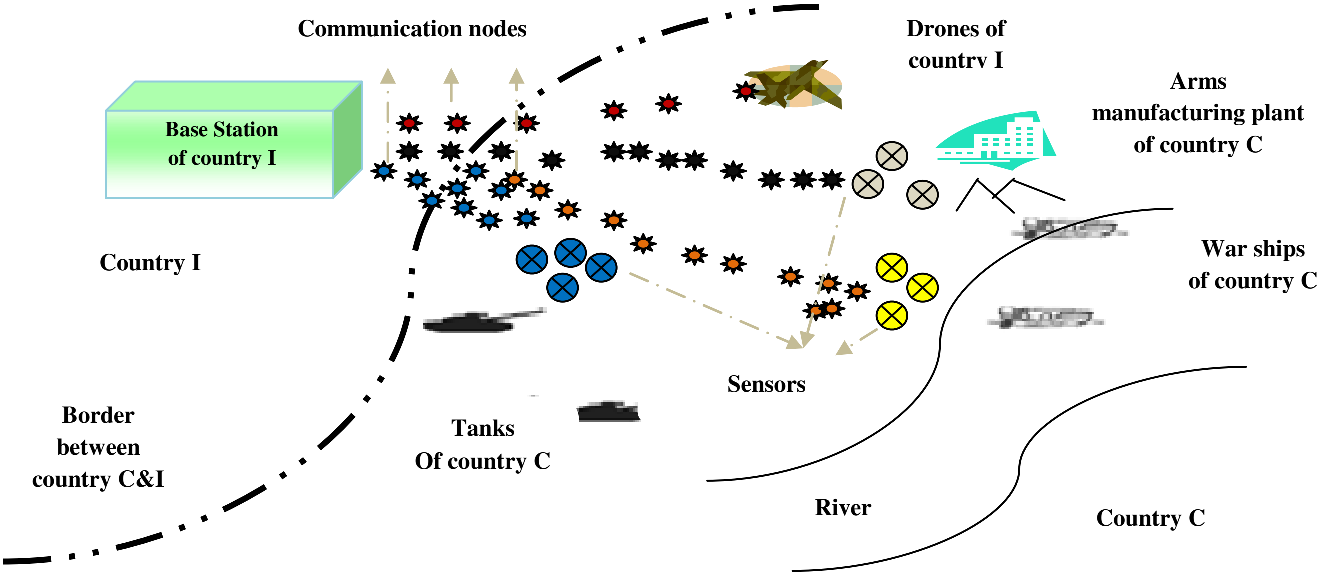


Figure 10.13 : Border Security Surveillance

The defense system of country I may face the threat of foreign computer hackers who can dismantle the power grid, transportation system, financial networks and e-governance system. The adversaries may try to gain control of critical switches; may

derail passenger trains, contaminate the water supply in major cities or shut down the power grid. Actually, country I requires new standards for critical public and private infrastructure facilities like power plants, water treatment plants and gas pipelines where a breach of security could cause significant economic damage. The recent wave of cyber attacks on various financial institutions and oil companies globally should be recalled in this context. A smart, resilient SCADA system can protect the critical infrastructure of a country through a set of efficient verification mechanisms. There is scope of future works on miscellaneous web security issues.

Security Intelligence Verification Mechanism [SIVM$_D$]
***System*: Defense SCADA;**
***Input* : Sensor data;**
***Move* : Call deep analytics → assess threats on 7-'S' elements;**

- **Scope : Private defense communication;**
- **System : Information system associated with SCADA such as computing, networking, data, application and security schema;**
- **Structure : Sensors (e.g. mobile sensors - drones, Unmanned Aerial Vehicle [UAV], static sensors – CCTV camera), base station server, communication channel;**
- **Strategy :**
    - **Governance :**
        - **proactive approach**
        - **reactive approach**
    - **Automated system verification and model checking**
    - **Shared vision on privacy and revelation principle**
    - **Intelligent communication protocol for collaborative and collective intelligence**
- **Security : audit security intelligence at multiple levels L$_{1\text{-}5}$;**
- **Staff: System administration, technical and maintenance staff, operation team;**
- **Skill : technical (e.g. electronics, communication, computer, electrical, mechanical), management information system, system maintenance, military operation;**
- **Style : Dynamic leadership style for efficient system coordination;**
- **Support: preventive and breakdown maintenance.**

***Revelation principle*: Audit privacy and confidentiality of critical data based on information disclosure policy.**
***Payment function*: Audit business intelligence of contracts with the vendors and service providers.**
***Verification algorithms* [refer section 9.4]:**

1. **Call threat analytics → assess threats on private defense communication channel;**
2. **Adopt risk mitigation strategies to ensure private defense communication :**
    - **Proactive approach**

        - **Call predictive analytics → analyze probability of occurrence vs. impact;**
        - **Call challenge-response protocol;**
    - **Reactive approach : interleaved hop-by-hop authentication; Adaptive security for dynamic data protection through preventive, detective, retrospective and predictive capabilities.**
    - **Sense-and-respond against bad luck such as natural disaster, military revolution, political strike, accidents and terrorism.**

3. Verify security intelligence of data, computing, application, networking and security schema of

defense SCADA at levels 1,2,3,4 and 5.

Level 1 (data schema):

- **Detect flaws in access control : confidentiality, data integrity, non-repudiation; authentication, authorization, correct identification, privacy and audit; false data injection attack;**
- **Intrusion detection;**
- **Compromising data warehousing, data mining, data visualization and performance measurement strategy;**

Level 2 (computing schema):

- **Correctness of computation**
- **Fairness in resource allocation**
- **Transparency of process, procedure and mechanism**
- **Accountability of role in system administration, operation and maintenance**

Level 3 (application schema):

- **Poor system performance : Denial of Service (DoS) attack, reliability, consistency, resiliency, liveness, deadlock, human error in remote operation of drones;**
- **Flaws in web application schema (e.g. session hijack, application integration);**

Level 4 (networking schema): Assess the risk of coremelt attack causing traffic congestion, delay in communication due to forward, blackhole, neighbor and jellyfish attack, cyber, rubber hose, sybil, node replication and wormhole attack;

Level 5 (security schema):

- **Assess the risk of multi-party corruption of one or more entities involved in private defense communication (e.g. sender, receiver, data, communication channel, mechanism and protocol) by adversaries;**
- **Assess the risks of *insider attack***
    - **Ensure privacy of the route and time of travel of the military convoy without any leakage of information.**
    - **Different time of travel of military and civilian convoy without any mix of the two traffics.**
    - **A pilot convoy should audit and check the clearance of route through drones.**
    - **Decomposition of a large convoy into smaller units**
    - **Intrusion detection through detectives and countermeasures**

- **Be alert on false data injection attack.**
- **Execute DoS attack on communication services to restrict false data injection attack (if necessary)./*caution : violation of human rights in healthcare and emergency services*/**

***Output*: security intelligence of defense communication network.**

Security Protocols

Intrusion Verification Mechanism

```
System : SCADA states (local, global, initial, goal), state transition relation;
Input : A self-set $S \subseteq U$, a monitoring set $M \subseteq U$ for a given system parameters;
Output: for each element $m \in M$, either self or non-self, danger or normal;
$D \leftarrow$ set of detectors that do not match any $s \in S$;
for each $m \in M$ do
        {
        call threat analytics (A) → sense danger signal ;
        secure function evaluation → verify innate and adaptive system immunity (i) = f(a,b,c,d,e);
        check e-passport, computing, storage and resource capacity in real-time;
        }
sense-challenge-respond to system immunity resiliently;
if m matches any detector $d \in D$ then identify m as non-self;
else identify m as self;
check if non-self  suspicious node is benign or malign danger node;
if it is malign then suppress it else give alert.
```

AI Moves :

a. *Multidimensional view of intelligent reasoning* (logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative, perception);

b. *Define system immunity* (i) = f(a,b,c,d,e); a: collective intelligence, b: machine intelligence, c: security intelligence, d: collaborative intelligence, e: business intelligence; f: secure verification function.

c. *Private search for evidence*;

An intrusion is considered as an activity that violates the security policy of a system. Intrusion detection systems are based on the assumption that the behavior of an intruder is different from that of an authorized user and the unauthorized activities can be detected by analyzing user's profile and activities, host based IDs, network based IDs and application based IDs. Auditing is required at different levels of granularity for the detection of misuse and anomaly. An intruder tries to gain access to an unauthorized system to which it has no legitimate access. It occurs by exploiting system vulnerabilities or by simply cracking the user ids and passwords of legitimate users. If a malicious agent is able to access the system, it is considered as an authorized user and is granted the access rights of the user. The basic objective is to effectively detect and prevent insider misuse. Intrusion may occur in various forms on a distributed network such as sybil, cloning or node replication,

wormhole denial of service, key interception and node capture. The following section presents intrusion verification mechanism (IVM).

Private Communication

Defense SCADA System architecture **: MTU: Defense base station i.e. master terminal unit; u: Communication nodes of defense network; v: sensor nodes; L: Leader of a cluster of sensor nodes; n: Number of hops between MTU and L; u_i: Upper association node; u_j: lower association node; k_u: Signcryption key of node u shared with MTU; k_{uv}: Pairwise signcryption key shared between nodes u and v; k^t_v: Time-stamped authentication key of node v; M (k,m) : Authenticated message m signcrypted with a key k.**

call challenge response protocol for *device attestation* verification → check whether a sensor node is tampered by a malicious agent;
check the *configuration* and correct setting of each sensor node → detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code;
check state variables and measure bad data against *false data injection* attacks; verify authentication in private communication between sensor nodes and base station or MTU;
do network traffic congestion analysis → assess the risk of *coremelt* attack;
do *multicast* traffic analysis → detect rushing, blackhole, neighbor and jellyfish attacks; check group, forward and backward privacy in secure group communication.

Let us consider test case 3 of private defense communication. It is very important to verify the privacy and security in SCADA communication. A malicious agent can exploit the configuration of a defense network to launch false data injection attack against state estimation and introduce arbitrary errors into certain state variables while bypassing existing techniques for bad measurements detection. Reliable SCADA operation requires system monitoring based on precise measurements of bus voltage, real and reactive power. These measurements are transmitted from the measuring instruments to SCADA. State estimation is used in system monitoring to estimate the best state by analyzing measured data and various system models. The output of the state estimation is used in contingency analysis. A malicious agent can compromise the measuring instruments to inject errors. Here, the real challenge is to detect bad measurements. If the malicious agent knows SCADA configuration, it can systematically generate bad measurements which can bypass the common assumption that the square of difference between observed and estimated data becomes significant during bad measurements. The attacker may try to inject arbitrary errors in certain state variables or aims to find an attack vector as long as it can result a wrong estimation of state variables. Real-time system monitoring is essential to ensure reliable operations of SCADA against false data injection attack. The adoption of communication equipments manufactured by foreign vendors may be a risky option in secure communication; it is an open debatable issue.

Device attestation verification is a critical requirement of a smart SCADA. It securely ensures whether a sensor node or remote terminal unit or any other device associated with SCADA network is tampered by a malicious attack. Each device should be attested with a valid digital test certificate. This certificate indicates the identity of the manufacturers, model number, serial number and tampering status of each device. SCADA must verify the identity and tampering status of each associated device. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of each device. The digital test certificate defines the basic security requirements of service provider and device manufacturer in terms of mutually acceptable security policies, certificate formats, naming convention and operational issues [18]. It should aid the deployment of system, operation, system audit, signing and revocation of certificate. Each device should be able to authenticate and authorize other devices without the support of backend security server. A malicious agent may be able to compromise a set of remote terminal units; it may be able to access the compromised RTUs and may launch a coordinated attack by modifying the software of the RTUs. It is also possible for the attacker to hide the attack by reporting correct data to the master terminal unit.

CSVM assumes that SCADA control center knows the exact hardware configuration of the sensor node or RTU like CPU model, CPU clock speed and the memory configuration. The hardware of the RTU is not corrupted. There is a secure authenticated communication channel between RTU and external verifier. The adversary can control the software and the operating system of RTU; it can access RTUs directly over the Internet or by compromising different devices of SCADA control center. There is at least one trusted external verifier at the SCADA control center which cannot be compromised by the malicious attacker.

A challenge response protocol is employed between a trusted external verifier and RTU. The external verifier sends a random challenge to the RTU. A self checking verification function on RTU computes a checksum over its own instructions and returns the result to the external verifier. If an adversary tampers with the verification function, either the computed checksum will be incorrect or there will be significant increase in computation time. If the external verifier receives the correct checksum within the expected time, it is concluded that the verification function code on RTU is unaltered. The verification function includes a cryptographic hashing function which computes a hash of RTU's memory. The external verifier compares the computed hash with the expected hash to ensure that the device has not been modified. Alternatively, a hash may be computed over a known executable to ensure that it has not been modified.

***False data injection attack*: The verification mechanism starts with a*uthentication certificate allocation.* SCADA administrator assigns each sensor and communication node an authentication certificate which is a unique ID endorsed with a bootstrapping time. Next step is *neighborhood search.* After the deployment in SCADA network, each new node handshakes with each of its neighbors by establishing a one-hop pair wise signcryption key. Each sensor node handshakes with the leader (L) and each communication node handshakes with the leader / other communication node / MTU. A node validates the IDs and time-stamps of its**

associated nodes with the help of MTU periodically. Then q number of sensor nodes *sense* the process variables collaboratively when they detect the occurrence of an event of interest. The leader collects the signcrypted data from all participating sensor nodes; unsigncrypts the signcrypted data; wraps them into a message (m) and forwards m to MTU through a set of communication nodes. Next step is relay; each forwarding communication node verifies the message code computed by its lower association node and then unsigncrypts the received message. If the verification fails; it drops the message and informs the instance to MTU. Otherwise, it computes a new message code based on its pairwise signcryption key shared with its upper association node. Finally, it forwards the message to the next node towards MTU. Finally, MTU verifies the message received from the communication node. If MTU detects that q nodes have endorsed the message (m) correctly, it accepts m otherwise discards m.

The basic objective of CSVM is to authenticate each communication node in the SCADA and also to know other valid communication nodes (neighbors) present in the system. A time stamp is involved in the authentication mechanism. The base station system administrator (SA) of SCADA network allocates a certificate to each node and it includes both ID and bootstrapping time to authenticate the identity of a new node. In the certificate, the ID and timestamp are signed by the private key of SA. When a new node is deployed in the SCADA, it shows its certificate to its neighbors. The neighbors can verify the certificate of the new node with the public key of SA. A new node can be accepted into the SCADA if it has a correct identity and a valid time-stamp.

Next, let us consider *Coremelt attack* where the malicious attackers send traffic between each other and not towards a victim host. It is a powerful attack since there are O(N^2) connections among N attackers which can cause significant congestion in core SCADA network. SCADA networks often use web service to enable coordination among physical systems. The malicious attackers are able to flood the end hosts with unwanted traffic to interrupt the normal communication. This is a specific type of Denial-of-Service (DoS) attack where the network link to SCADA server is congested with illegitimate traffic such that legitimate traffic experiences high loss and poor communication performance. Such a poor connectivity between SCADAs can damage critical infrastructure with cascading effect. To address such attacks, it is important to identify the source of excessive traffic and prioritize legitimate traffic. The attackers often rely on distributed denial of service attacks where many subverted machines i.e. botnets are used to generate illegitimate traffic. There are three steps to launch a Coremelt attack [25]. First, the attackers select a link in the SCADA network as the target link. Then, they identify what pairs of subverted machines can generate traffic that traverses the target link. Finally, they send traffic between the identified pairs to overload the target link. Thus, the attacker uses a collection of subverted machines sending data to each other to flood and disable a network link. An efficient SCADA should allow end hosts to identify long-running legitimate traffic. During heavy load, the router forward packets with proper priority and capabilities while dropping packets without capabilities. SCADA requires an efficient tracing and network traffic monitoring system to avoid this attack.

Next let us discuss *multicast attack.* The communication schema of SCADA should support message *broadcasting* and *multicasting*. SCADA may have thousands of sensor nodes or remote terminal units. Therefore, multicasting is a critical requirement of secure SCADA communication. The number and size of keys to be stored in a remote terminal unit should be limited due to memory constraint. The computational and communication cost is O(n) where n is the number sensor nodes or remote terminal units. In SCADA network, actual addition or deletion of a sensor node occurs rarely since the system is commissioned based on a long term plan. But, the remote nodes may be easily compromised by the malicious agents. It needs an efficient *key management mechanism* to preserve group key, forward and backward privacy [15,16]. *Group key privacy* is computationally infeasible for an adversary or malicious agent to discover any group key of SCADA. *Forward privacy* prevents a user which has already left from the SCADA group from accessing future communication within the group all the keys along the path from the leaving point to the root node of the key tree should be changed. It ensures forward privacy. *Backward privacy* prevents a user from accessing past communications of SCADA group, all the keys along the path from the joining point to the root node of the key tree should be changed. The protocols for key management of secure group communication such as join, leave and sub-group change can be found in [37,38,39].

Web Security Verification

***Application*: Web enabled SCADA; Agents: User of the web application, system administrator;**

verify the *design flaws* in service oriented computing schema.

***logic attack* : check the main flow, sub flows and exception flows as per business rules of the application;**

***cross site scripting*: check whether all parameters of the web application are validated properly; check the risk of phishing attack;**

***injection flaws* : check whether user data modify the meaning of command and queries sent to any interpreters invoked by web application;**

***malicious file injection* : check the use of dangerous application programming interfaces by testing and code review;**

***insecure direct object reference* : check through code review whether the web application allows direct object references;**

***cross site request forgery* : check whether web application generates authorization token that is not automatically submitted by the web browser;**

***information leakage and improper error handling*: check whether web application leaks any data through error messages; check whether the application builds a trusted computing environment;**

***broken authentication and session management*: check through code review whether the web application properly authenticates users and protects their identities and credentials;**

***insecure cryptographic storage*: check whether web application properly encrypts sensitive data; check configuration of the web server;**

insecure web communication: **check whether the web application ensures private communication between the sending and receiving agents; assess the risk of snooping;**

failure to restrict URL access **: check whether proper access control is enforced at the presentation layer and business logic for all URLs in the web application;**

The web security verification mechanism (WSVM) verifies service oriented computing schema to mitigate the risk of common vulnerabilities. WSVM addresses a set of dangerous attacks against web enabled distributed computing system. The basic objective of WSVM is to protect SCADA from phishing attacks, privacy violations, identity theft, system compromise, data alternation, data destruction, financial and reputation loss. Cross site scripting (XSS) flaw allows an attacker to execute malicious code in the web browser of the user that can hijack user session, deface websites, possibly introduce worms or insert hostile content or conduct phishing attack and take over the browser of the victim through malware. The best protection of XSS is a combination of validation of all incoming data and appropriate encoding of all output data. Validation allows the detection of XSS attacks and encoding prevents injection of malicious script into the browser. Cross site request forgery (CSRF) forces the web browser of the logged on user to send a request to a vulnerable web application which forces the victim's browser to perform a hostile action. Web applications rely solely on automatically submitted credentials such as session cookies, basic authentication credentials, source IP address, SSL certificates or windows domain credentials. CSRF is applicable to any web application that has no authorization checks against vulnerable actions.

Injection flaws allow the attacker to create, read, update or delete any arbitrary data available to the application. Even, it may compromise the web application completely bypassing firewalled protection. SQL injection occurs when the data input of the user is sent to an interpreter as part of a command and query. The hostile data of the attack forces the interpreter to change the data or execute unintended command. The common protection measures are to use strong and safe interpreters, do input validation, use strongly typed parameterized query APIs, enforce least privileges, avoid detailed error messages, use stored procedures, do not use dynamic query interfaces and do not use simple escaping functions.

Web application developers often trust input files improperly and the data is checked insufficiently. Arbitrary, remote and hostile content may be processed or invoked by the web server. It allows an attacker to perform execution of malicious code, installation of tool kit and system compromises remotely. Flawless design is required during the construction of system architecture, design and software testing. The application developers should use indirect object reference map, check errors, validate user's input and implement firewall rules appropriately. Another critical problem is insecure direct object reference; a direct object reference occurs when a reference is exposed to a file, directory, database records or key as a URL or form parameter. A malicious agent can manipulate these references to access other objects without authorization. The web application should avoid exposing direct object reference to the users by using an index, indirect reference map or other indirect validated method that is easy to validate.

An web application can unintentionally leak information about their configuration, internal state or violate privacy through error messages and it can launch dangerous attacks. The application should get support from a standard exception handling mechanism to prevent the leakage of unwanted information; detailed error handling should be limited; errors should be properly checked and should not be exploited by the intruders. Broken authentication and session management is caused due to the failure of protection of credentials and session tokens. It can hijack user's or administration's accounts, undermine authorization and accountability controls and cause privacy violations. The common protective measures are the adoption of efficient authentication mechanisms, secure communication and credential storage, use of efficient session management mechanisms; invalid session identifiers should be rejected.

Insecure cryptographic storage is caused due to the failure in encrypting sensitive data; it leads to disclosure of sensitive data and compliance violation. It is required to avoid inefficient weak cryptographic algorithms and check whether sensitive data are encrypted properly. An web application may fail to encrypt network traffic to protect sensitive communications. The adversary can sniff traffic from the communication network and access sensitive data, credentials, authentication or session token. The application should properly encrypt critical data. The only protection for a URL is that links to a page are not presented to unauthorized users. The adversary may get access to these pages and view private data. All URLs and business functions should be protected by an effective access control mechanism. Web security is a very broad topic; some common critical issues have been discussed above very briefly. There are several open issues in the design of service oriented computing schema. It is an interesting option to interview Internet experts, web developers and programmers and analyze the complexities and challenges in web programming issues.

Access Control

Biometrics are used for automated recognition of SCADA users and system administrators based on their biological and behavioral traits such as finger prints, face image, iris and voice. Traditional authentication methods like passwords and identity documents may fail to meet reliable security and performance of identification systems. Some physical and behavioral attributes of human beings are uniquely associated with an individual. Biometrics captures these traits with sensors; represent them in digital format; compare the recorded data with the data acquired from the same user previously and performs recognition [33]. Biometrics are applicable to VISA verification for regulating international border crossing, welfare distribution, access control at airport and power plant's control room, access control to shared resources and information, remote financial electronics transactions and distribution of social welfare benefits.

SCADA may be attacked at any point such as host or MTU, RTU, communication node or sensor node. It should be protected by a robust access control mechanism. Access control is the process of receiving the requests of the users for specific resources and data and determining whether the request should be granted or denied. The access control system is a combination of access control policy, model

and mechanism. Access control may be based on user's identity or role or the regulatory constraints as defined by the system administrator. Credential based access control grant or deny access to the resources by exploiting digital certificates and make access decisions on the basis of a set of properties that the client should have fulfilled. This trust negotiation process may suffer from privacy problem since the SCADA server discloses its access control policy entirely and the client exposes its credentials certificates to gain access to a resource. An efficient negotiation strategy should restrict the disclosure of information. The service accessibility rules specify the necessary and sufficient conditions for accessing a resource while credential disclosure rules define the conditions that govern the release of credentials and declarations. The SCADA server should discloses the minimal set of policies for granting access while the client releases the minimal set of certificates to access the resource. Prerequisites are the conditions that must be satisfied for a service request. Requisites are conditions that allow the service request to be successfully granted. The SCADA server should not disclose a requisite rule until the client satisfies a prerequisite rule. Biometrics can be also used for credential based access control of distributed computing systems.

```
Agents: Client (C), SCADA server (S);
check the correctness of enrollment and recognition mechanisms for biometric access control;
    C requests S for the access to a resource r such as data or application;
    S requests C for prerequisites;
    C informs prerequisites to S;
    S requests for requisites to C;
    C informs requisites to S;
    S verifies the credentials provided by C;
        if the verification is true, then S grants C the access to r;
        else S asks C the required credentials;
            C selects the requested credentials (if possible) and informs S;
            S verifies the credentials of C;
                if the verification is true, then S grants C the access to r;
                else S rejects the request of C;
```

intrinsic failure: check false match, non-match and failure to enroll or acquire biometric data;
adversary attacks: check collusion, coercion, negligence, enrollment fraud, exception abuse;
infrastructure attacks: check sabotage overloading, attacks on user interface, system modules, databases and interconnections, modification of data and information leakage, spoofing, impersonation, man in the middle attack, replay and hill climbing.

Credential based access control strategy grants or denies access to the resources based on biometric prerequisites and requisites as specified by the client during trust negotiation process.

BACVM mechanism verifies the security intelligence of a biometric access control system associated with SCADA. It basically explores the risks of various threats on biometric access control. A *User* presents his or her biometric identity to a biometric system for the purpose of being recognized. Biometric systems can be used efficiently for authentication, nonrepudiation and identity recognition claim. Biometric recognition is the science of establishing the identity of the user based on his or her physical and or behavioral characteristics either in fully automated or a semi-automated way. A biometric system measures one or more physical or behavioral traits such as finger print, palm print, face, iris, retina, ear, voice, signature, gait, hand vein, odor or DNA information of an individual to determine or verify his identity. These characteristics are known as traits, indicators, identifiers or modalities. The biometric mechanism has two phases – enrollment and recognition. During enrollment, biometric data is acquired from the individuals and stored in a database along with the person's identity. During recognition, biometric data is acquired from the individual and compared with the stored data to determine the identity of the user.

The failure to a biometric system is basically a security threat - denial of service (DoS), intrusion, repudiation and function creep. The legitimate users may be prevented from obtaining access to the information assets. An unauthorized user may gain illegitimate access to the system and this intrusion affects the basic integrity of the system. A legitimate user denies the usage of system or data after having access to it. Corrupted users may deny their actions. An adversary may exploit the biometric system for different function. The biometric system may fail due to flaws in enrollment and recognition mechanisms. It may also fail due to manipulation by adversaries which could either be insider or external entities. External entities may be imposters and attackers. Insiders may be system administrators or legitimate corrupter users. Insider attacks may be collusion, coercion, negligence, enrollment fraud and exception abuse. Infrastructure attacks may be due to sabotage overloading; it may be attacks on user interface, system modules, interconnections and template databases. Attacks on user interface result impersonation spoofing alternation. Attacks on system modules cause modification and exploit faults. Attacks on interconnections cause man-in-the-middle, replay or hill climbing. Attacks on template database result modification and leakage of critical sensitive data.

An adversary may attack human element or system infrastructure associated with a biometric system. The system administrators may do mistakes in enrollment, disenrollment of users or in adjustment of security parameters controlling the performance of a biometric system such as threshold on match scores and minimum limits on the quality of acquired biometric sample. The administrator may do mistakes and breach the security of biometric system. In case of collusion, an authorized user willingly turns malicious and attacks the system either individually or in collaboration with external adversaries. A coerced user does not carry out any attack willingly. An authorized user is forced to turn malicious through physical threat or blackmail. External attackers can also exploit the negligence of authorized users such as log out of the system after completing transactions. In case of enrollment fraud, an adversary may be able to enroll into the biometric system

illegally with a false identity and credentials. The system administrator should detect a duplicate identity by matching the biometric traits of a new user against the traits of all enrolled users. Another critical issue is exception abuse where exceptional situations may cause denial of service to legitimate users. It may be the failure of hardware and software components of a biometric system or poor quality of data (e.g. noise, missing data) during enrollment phase.

An adversary may attack the functional modules of a biometric system infrastructure such as sensor, extractor, template database, matches or attacks at the interface of the modules and decision modules. The common types of attacks are overloading and sabotage. A malicious agent may cause physical damage to one or more components of the biometric infrastructure such as putting off power supply, damaging of sensor interfaces or introducing excessive noise that affects the normal operation of biometric system. An imposter may attempt to intrude the biometric system by posing himself as an authorized user either casually or targeted way. The imposter does not modify his biometric traits in the first case. In the second case, the imposter may target an identity whose biometric characteristics are known to be similar to its traits. The imposter may execute mimicry attack by modifying his biometric characteristics. It may adopt the strategy of obfuscation by changing biometric characteristics to avoid detection. It is mainly applicable in negative recognition applications. Obfuscation can be done by presenting a poor quality image or noisy biometric sample. The solution is to improve the robustness of biometric algorithm.

Spoofing is the most common attack at user interface level and it involves the presentation of spoof biometric trait. A spoof is any counterfeit biometric that is not obtained from a live person. It includes the presentation of fake or artificial traits such as gummy finger, thin film on the top of a finger, recorded voice or mask of a face. If the sensor is unable to distinguish between spoofed and genuine biometric traits, an adversary can easily intrude the system under a false identity. Spoof detection is done through liveness detection by checking the signs of human vitality or liveness through blood pulse. Spoofing can be done by directly colluding with or coercing an authorized user, covert acquisition, hill climbing attacks or stealing the biometric template from the database. For spoof detection, common psychological properties used include pulse rate, blood pressure, perspiration, spectral or optical properties of human skin, electrical conductivity of human tissues and skin deformation. A malicious agent can subvert biometric processing by directly undermining the core functional modules of a biometric system such as signal processing or pattern making algorithms or by manipulating the communication between these modules. Template database can be hacked or modified by an adversary to gain unauthorized access or to deny access to legitimate users. There may be leakage of stored biometric template information due to lack of strict database access control.

The biometric system is a costly option in information security management; it requires complex data schema in terms of data warehousing and data structure. It ensures non-repudiation authentication and integrity, only legitimate or authorized users are able to access physical or logical resources protected by it. The imposters cannot access the protected resources or information. Another important issue is

availability where authorized users must have timely and reliable access to the protected data. It also ensures confidentiality; it must be used for the intended functionality i.e. credential based access control. A user can be recognized by what he knows (e.g. passwords, PIN or cryptographic key), what he possesses (e.g. passport, driving license, mobile phone, ID card) and who he is intrinsically (e.g. inherent physical and behavioral characteristics). The proliferation of web based services and deployment of distributed computing systems have led to the risks of identity theft significantly. Facial recognition software, voice recognition system and digital fingerprint or palms scanning are emerging trends of biometrics. The traits such as fingerprints, retina, vein patterns and facial dimensions are generally considered unique user profile but these features may be associated with a fake user ID intentionally or by mistake during registration process. Biometric data management should take care of user privacy and institutional convenience simultaneously.

Privacy Verification

***Agents*: Client (C), SCADA / ICS administrator;**

***Input*: Query for sensitive sensor data (q);**

***Output* : Private sensor data (d^p_s);**

C→SCADA: q;

SCADA: Retrieve sensor data (d_s); Call move (M_i) for privacy preserving data mining;

- **M_1: Suppress d_s partially;**
- **M_2: Randomize d_s;**
- **M_3: Achieve k-anonymity through generalization, suppression, de-identification;**
- **M_4: Summarize or aggregate d_s;**
- **M_5: Replace d_s with a small sample;**
- **SCADA→ C: d^p_s ;**

Verify the performance and efficiency of algorithms: encryption, decryption, digital signature, digital certificate, signcryption;

Verify the degree of information leakage in inference control.

PVM preserves the privacy of SCADA data through efficient secure multi-party computation and privacy preserving data mining.

A client interacts with SCADA through enterprise applications or web; submits simple or complex queries and searches for intelligent information. A malicious agent may be able to attack SCADA server during this communication between sending and receiving agents. PVM tries to protect sensitive data from unsolicited or unsanctioned disclosure of SCADA data by calling different statistical disclosure control and privacy preserving data mining techniques. The privacy of sensitive SCADA data may be preserved by suppressing the data intelligently before any disclosure or computation. Specific attributes of particular records may be suppressed completely. In case of partial suppression, an exact attribute value is replaced with a less informative value by rounding or using intervals. K-anonymity is achieved through generalization, suppression and de-identification [8]. The

attribute values are generalized to a range to reduce the granularity of representation. Quasi-identifier attributes are completely or partially suppressed. De-identification is achieved by suppressing the identity linked to a specific record or altering the dataset to limit identity linkage. Summarization releases the data in the form of a summary that allows approximate evaluation of certain classes of aggregate queries while hiding individual records. The sensitive data set may be replaced with a small sample. Aggregation presents data in the form of sum, average or count. Randomization perturbs the data randomly before sending them to the server and introduces some noise. The noise can be introduced by adding or multiplying random values to numerical attributes. SCADA administrator generally preserves the privacy of sensitive data through encryption, decryption, digital signature and certificates and signcryption. PVM checks whether different statistical disclosure control techniques are really able to preserve the privacy of sensitive SCADA data from the adversaries during communication with the client through web or different enterprise applications.

The next issue is the security of quantum computing model in depth. At level L1, is it possible to verify the efficiency of access control in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, non-repudiation and data integrity? For any secure service, the system should ask the identity and authentication of one or more agents involved in secure multi-party computation. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries.

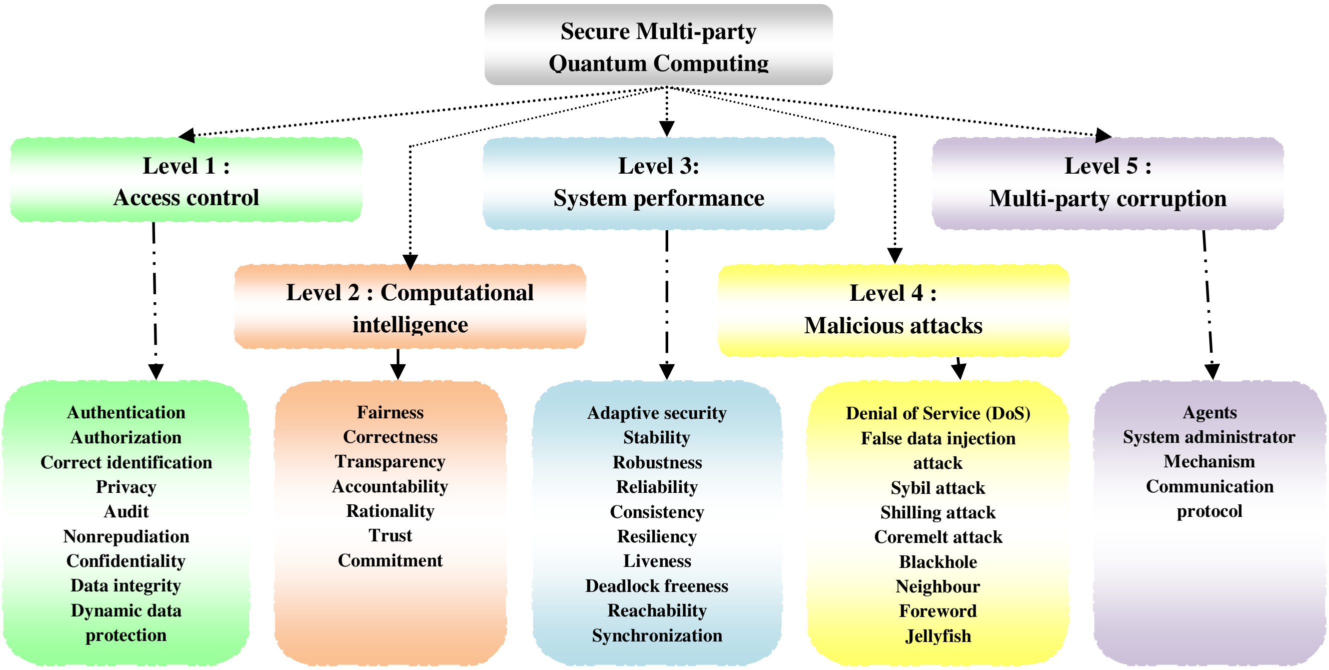


Figure 10.14: Secure Multi-party Quantum Computing

After the identification and authentication, quantum computing model should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication.

Privacy is a critical concern of the revelation principle of quantum computation; is it possible to address the issue of secure private communication through cryptography, digital signature and signcryption? The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption methods. Data integrity ensures that data is protected from unauthorized modifications or false data injection attack. The system should provide public verifiability so that anyone can verify the integrity of the data. Redundancy of data is a critical issue which is resulted through replication across the writers.

Traditionally, cryptographic solutions are focused to ensure information security and privacy. Is it possible to explore other different security concerns of quantum computing model? At level L2, is it possible to verify the efficiency of secure multiparty quantum computing in terms of fairness, robustness, correctness, transparency, accountability, trust and commitment? A protocol ensures correctness if the sending agent broadcasts correct data and each recipient receives the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with the commitment, honesty and rational reasoning on payment function, trust and quality of service. Fairness ensures that something will or will not occur infinitely often under certain conditions. The recipients expect fairness in private communication according to their demand plan, objectives and constraints. The sending agent expects fairness from the recipients in terms of true feedback and commitment on confidentiality of data. As per traditional definition of fairness of secure multi-party computation, either all parties learn the output or none. The system must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. In fact, accountability is also associated with collective intelligence. Transparency is associated with communication protocols, revelation principle and automated system verification procedures. For example, a mechanism should clearly state its goal to define a policy. There exists an inherent tension between transparency and privacy. A fully transparent system allows anyone to view any data without any provision of privacy. On the other side, a fully private system provides no transparency. Privacy can be achieved using cryptographic techniques at increased cost of computation and communication. Is it possible to trade-off privacy vs. transparency? Is it possible to provide public verifiability of its overall state without

disclosing information about the state of each entity? Public Verifiability allows anyone to verify the correctness of the state of the system.

Next, is it is possible to verify the system performance of quantum computing model at level L3 in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety? The performance of a system and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Safety is a critical requirement of any system whether it may be mechanical, electrical, electronics, information technology, civil, chemical, metallurgical or instrumentation engineering. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. Another important issue is robustness of a system. The delivery of the output should be guaranteed and the adversary should not be able to threaten a denial of service attack against a protocol.

At level L4, is it possible to assess the risks of various types of malicious attacks by adversaries on quantum computing model such as Denial of Service (DoS), false data injection attack, sybil attack, shilling attack, coremelt attack (or network traffic congestion), blackhole, neighbor, node deletion, rushing and jellyfish attacks? A quantum computing model may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. Quantum computing model demands the support of an adaptive security architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of quantum computing that monitors it in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. At level L5, it is required to assess the risks of various types of corruptions of the agents associated with quantum computing model.

Let us explain the objectives of adaptive security of quantum computing model in depth. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for the emerging technologies. The systems demand continuous monitoring and remediation; traditional 'prevent and detect' and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach. For example, prevention and detection are traditional approaches to the security of a system. In today's world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security

but should adopt cloud based solutions and open application programming interfaces also. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture.

Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjust individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of the system and complexity of networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

Security Analytics:

***Agents* : System analysts;**

A*lgorithm*:

- ✪ **call intelligent threat analytics, verify security intelligence at multiple levels.**
  - ***Level 1*: audit computational intelligence in terms of correctness of computation and rationality of filter configuration,**
  - ***Level 2*: verify system performance of the adaptive filter in terms of reliability, consistency, resiliency and liveness;**
  - ***Level 3*: malicious attacks – verify the risks of Denial of Service (DoS), false data injection, intrusion and Sybil attack on adaptive filter;**
  - ***Level 4*: multi-party corruption - assess the risks of corruption of system administrator and filtering mechanism of adaptive filter;**
  - ***Level* 5: verify the efficiency of access control of adaptive filter in terms of authentication, authorization, correct identification, privacy, audit, nonrepudiation, confidentiality and data integrity.**
    - ***Revelation principle* : Preserve privacy of output of adaptive filter.**
- **identify what is corrupted or compromised?**
- **time : what occurred? what is occuring? what will occur? assess probability of occurrence and impact.**
- **insights : how and why did it occur? do cause-effect analysis.**

- **recommend : what is the next best action?**
- **predict : what is the best or worst that can happen?**

What do you mean by security in adaptive filter; how to verify security intelligence in adaptive filter? It is essential to verify security intelligence of secure adaptive filter collectively through rational threat analytics at five levels : L1, L2, L3, L4 and L5. The basic building blocks of the security of adaptive filter are an adversary model and an intelligent threat analytics. An adversary is a malicious agent who attacks a system or a protocol; the basic objectives are to cause disruption and malfunctioning of a secure system. The security intelligence of adaptive filter should be analyzed in terms of assumptions, goals and capabilities of the adversary. It is also crucial to analyze the adversary model in terms of environment, location, network, resources, access privileges, equipments, devices, actions, results, risks, reasons and motivations of attacks and probable targets (i.e. why the adversary attacks and to obtain what data).

Theorem : ***Correctness and privacy of computation of adaptive filter is ensured through a rational threat analytics.***

It is essential to verify correctness and privacy of computation by the adaptive filter. The correctness of the filter is deeply associated with right configuration of the data schema (S). The privacy of computation can be ensured through a robust revelation principle of the filter. The data schema (S) may be misconfigured due to various types of threats such as Sybil attack, false data injection attack, shilling attack by corrupted recommender system and multi-party corruption. In case of false data injection attack, incomplete, corrupted, noisy and incorrect data may be fed to the data schema (S). It is essential to verify the fairness, trust and correctness of input data in time.

It is really complex to trace the corrupted agents. The entities associated with the data schema (S) may be partitioned into two subsets: correct and faulty. Each correct entity presents one legitimate identity to other entities. Each faulty entity presents one legitimate identity and one or more counterfeit identities to S. Each identity is an informational abstract representation of an entity that persists across multiple communication events. The entities communicate through messages. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt the data schema (S) that relies on redundancy by injecting false data or suppressing critical data. It is sybil attack. Sybil attack may be detected through intelligent tracing mechanism such as trusted explicit and implicit certification, robust authentication, resource testing and incentive based game.

It is essential to verify the security intelligence of adaptive filter at multiple levels to ensre the correctness and privacy of computation. At level L1, is it possible to verify the efficiency of access control in terms of authentication, authorization, correct identification, privacy, audit, confidentiality, non-repudiation and data integrity. For any service from the filter, the system should ask the identity and authentication of one or more agents involved in secure multi-party computation. The agents of the same trust zone may skip authentication but it is essential for all sensitive

communication across different trust boundaries. After the identification and authentication, an adaptive filter should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. The agents must commit the confidentiality of data exchange associated with private communication.

Privacy is a critical concern of the revelation principle of secure adaptive filter; is it possible to address the issue of secure private communication through cryptography, digital signature and signcryption? The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption methods. Data integrity ensures that data is protected from unauthorized modifications or false data injection attack. The system should provide public verifiability so that anyone can verify the integrity of the data. Redundancy of data is a critical issue which is resulted through replication across the writers.

Traditionally, cryptographic solutions are focused to ensure information security and privacy. Is it possible to explore other different security concerns of adaptive filter? At level L2, is it possible to verify the efficiency of adaptive filter in terms of fairness, robustness, correctness, transparency, accountability, trust and commitment? A protocol ensures correctness if the sending agent broadcasts correct data and each recipient receives the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with the commitment, honesty and rational reasoning of the associated agents on payment function, trust and quality of service. Fairness ensures that something will or will not occur infinitely often under certain conditions. The recipients expect fairness in private communication according to their demand plan, objectives and constraints. The sending agent expects fairness from the recipients in terms of true feedback and commitment on confidentiality of data. As per traditional definition of fairness of secure multi-party computation, either all parties learn the output or none. The system must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. In fact, accountability is also associated with collective intelligence. Transparency is associated with communication protocols, revelation principle and automated system verification procedures. For example, a mechanism should clearly state its goal to define a policy. There exists an inherent tension between transparency and privacy. A fully transparent system allows anyone to view any data without any provision of privacy. On the other side, a fully private system provides no transparency. Privacy can be achieved using cryptographic techniques at increased cost of computation and communication. Is it possible to trade-off privacy vs. transparency?

Next, is it is possible to verify the system performance of adaptive filter at level L3 in terms of stability, robustness, reliability, consistency, resiliency, liveness, deadlock freeness, reachability, synchronization and safety? The performance of a system and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. Another important issue is robustness of a system. The delivery of the output should be guaranteed and the adversary should not be able to threaten denial of service attack against a protocol.

At level L4, is it possible to assess the risks of various types of malicious attacks by adversaries on adaptive filter such as Denial of Service (DoS), false data injection attack, sybil attack, shilling attack, coremelt attack (or network traffic congestion), blackhole, neighbor, node deletion, rushing and jellyfish attacks? An adaptive filter may face various types of threats from both external and internal environments but it should be vigilant and protected through a set of security policies. An adaptive filter demands the support of an intelligent architecture so that the associated system can continuously assess and mitigate risks intelligently. Adaptive security is a critical feature of the filter that monitors it in real time to detect any anomalies, vulnerabilities or malicious traffic congestion. If a threat is detected, the technology should be able to mitigate the risks through a set of preventive, detective, retrospective and predictive capabilities and measures. Adaptive security analyzes the behaviors and events to protect against and adapt to specific threats before the occurrence of known or unknown types of malicious attacks. At level L5, it is required to assess the risks of various types of corruptions of the agents associated with an adaptive filter.

Let us explain the objectives of security of adaptive filter in depth. New threats are getting originated as an outcome of technology innovation and may cause new forms of disruptions with severe impact. Today, it is essential to deploy adaptive security architecture for the emerging technologies. The system demands continuous monitoring and remediation; traditional ‘prevent and detect’ and incident response mindsets may be not sufficient to prevent a set of malicious attacks. It is required to assess as-is system administration strategies, investment and competencies; identify the gaps and deficiencies and adopt a continuous, contextual and coordinated approach. For example, prevention and detection are traditional approaches to the security of a system. In today’s world of expanding threats and risks, real-time system monitoring is essential to predict new threats and automate routine responses and practices. The system should not only rely on traditional prevent-and-detect perimeter defense strategies and rule based security but should adopt cloud based solutions and open application programming interfaces also. Advanced analytics is the basic building block of next generation security protection which should be to manage an enormous volume, velocity and variety of data through AI and machine learning techniques. Intelligent analytics are expected to detect anomalous patterns by comparing with the normal profile and the activities of the users, peer groups and other entities such as devices, applications and smart

networks and trigger alarms by sensing single or multiple attacks on the system. The security element must overcome the barriers among security, application development and operations teams and be integrated deeply into system architecture. Next, it is essential to develop effective ways to move towards adaptive security architecture. The mechanism should surfaces anomalies and adjusts individualized security controls proactively in near real-time to protect the critical data of a system. Adaptive Security with dynamic data protection is expected to offer many benefits over traditional security platforms depending on the size of the system and complexity of networking schema – real time monitoring of events, users and network traffic; autonomous and dynamic resolutions; prioritization and filtering of security breaches; reduction of attack surface and impact or damage of a threat and reduction of resolution time. The emerging technology is expected to adapt to the needs of a system irrespective of the size of network, nature of operation or exposure of threats. It can assess the requirements of security with greater accuracy through a set of intelligent policies and procedures and can ensure better understanding of strength, weakness, opportunities and threats of the security architecture.

Let us also discuss the issue of private classification by secure adaptive filter using kernel method such as support vector machine. Private SVM returns outputs (e.g. kernel value, classification labels) in encrypted form so that the same can be decrypted only through a common agreement by authorized agents. SVM algorithm may reveal sensitive data in various ways. SVM may leak some side information that is not specified by functions of the algoritm. The specified output result itself can reveal sensitive data. Private SVM should define an intelligent revelation principle : which data can be revealed. It should not reveal more information than required. The basic building block of private SVM may be secure multi-party computation which can preserve the privacy of sensitive data through various methods : adding random noise to data [The basic objective of data perturbation is to alter the data so that real individual data values cannot be recovered. For an input x, (x+r) preserves the privacy of x if r is a secret random number]; splitting a message into multiple parts randomly and sending each part to a DMA through a number of parties hiding the identity of the source; controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication; dynamically modifying the sequence of events and agents through random selection; permuting the sequence of messages randomly and masking of data;

Let us consider the second issue - the output results generated by SVM may reveal sensitive information. There should be a trade-off between revealing sensitive information and useful knowledge. SVM can reveal internal value, classifier and classification results. Any of the revealed internal values can breach the privacy of training and testing data and the output results can also leak the privacy of classified data. Thus, it is important to define what additional information should the analysts come to know after running a private SVM; only an authorized agent should know class labels of classified data. If the classification results are too sensitive then the authorized agent should obtain only an aggregated output data. Private SVM assumes a semi-honest model the agents follow the protocol correctly

but use the obtained information to gain new knowledge. It should neither leak information training data nor the classifiers; the sensitive data should be encrypted. There should be a tradeoff between privacy and the efficiency of private SVM in tems of cost of computation and communication.

5. STRATEGY

Strategy Analytics

Prof. Simon Watson is exploring a set of intelligent strategic moves for the innovation of emerging digital technologies such as scope analysis, requirements engineering, system design, talent management, team management and coordination, resources planning, concept development, concept evaluation, system architecture design, system development plan, roll out, process design, prototyping and testing The technological innovation on digital technology is associated with. Efficient change management ensures that an organization and its workforce are ready, willing and able to embrace the new processes and information systems. The change management is a complex process. The change should occur at various levels such as system, process, people and organization. Communication is the oil that ensures that everything works properly. It is essential to communicate the scope of digital technology to the policy makers, state and central governments, corporate executives, academic and research community.

Strategy can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. Technology trajectory is the path that the technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. The emerging digital technologies are now passing through the growth phase of S-curve. Initially, it may be difficult and costly to improve the performance of the technology. The performance is expected to improve with better understanding of the fundamental principles and system architecture. The dominant design should consider an optimal set of most advanced technological features which can meet the demand of the customer, supply and design chain in the best possible way. It is really interesting to analyze the impact of various factors on the trajectory of digital technology

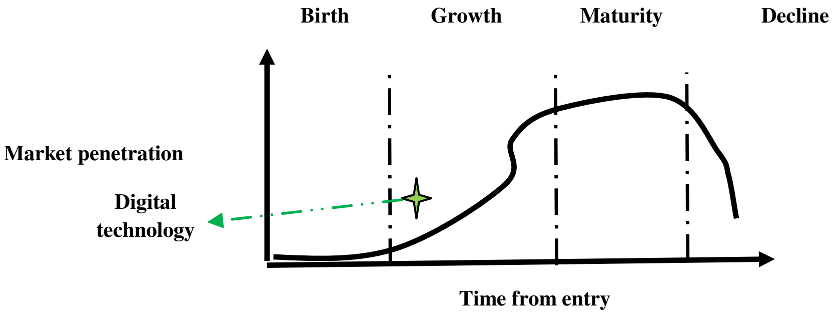


Figure 10.15: Technology life-cycle analysis

SWOT Analysis on Cloud Computing **: Let us exercise SWOT analysis on cloud computing. The strength of cloud computing is associated with several issues such as IT cost reduction, improved system performance and productivity, easier maintenance, agility, device and location independent access, scalability and elasticity via dynamic provisioning of resources in near real-time, security, multitenancy, availability, business continuity, disaster recovery, on demand self service (e.g. computing capabilities, server time, network storage capacity), broad network access by various client platforms (e.g., mobile phones, tablets, laptops, and workstations), resource pooling, rapid elasticity and measured services. Multitenancy enables sharing of resources and costs across a large pool of service consumers; the computing resources of the service provider can be pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned as per the demand of the service consumers. System capabilities can be elastically provisioned and released maintaining scalability automatically. Resource usage (e.g. storage, processing, bandwidth, active user accounts) can be monitored, controlled, optimized and reported with transparency. It is possible to ensure agility of an enterprise with re-provisioning, adding or expanding technological infrastructure resources. Cost reduction is possible by converting capital expenditure to operational expenditure. This strategy may lower barriers to entry as IT infrastructure is provided by a third party and need not be purchased for one time or infrequent intensive computing tasks.**

But, there are several limitations of cloud computing such as privacy of critical strategic data, loss of control over critical strategic data, access control problems, confidentiality, data integrity, reliability, consistency, resiliency, network traffic congestion, delay in data communication, threats of various types of malicious attacks (e.g. sybil attack, false data injection attack, denial of service attack) and multi-party corruption. The top three threats in the cloud are insecure interfaces and APIs, data loss, data leakage and hardware failure. Cloud computing poses privacy concerns as the service provider can access the data of service consumer in the cloud at any time. It could accidentally or deliberately alter or delete critical data. The service providers may share or sell strategic data of the consumers to third parties. The consumers can encrypt data to prevent unauthorized access. But, this move may result high cost of computation and communication.

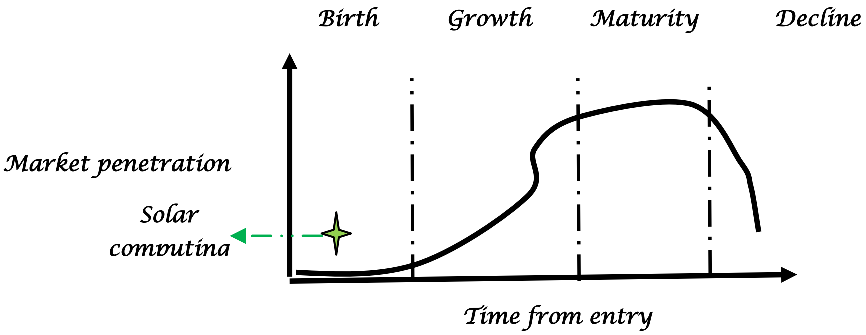


Figure10.16: Technology life–cycle analysis of solar computing

The technological innovation on a smart grid is associated with a set of intelligent strategic moves such as scope analysis, requirements engineering, quality control, system design, concurrent engineering, talent management, team management and coordination, resources planning, concept development, concept evaluation, system architecture design, system development plan, roll out, process design, prototyping and testing. Efficient change management ensures that an organization and its workforce are ready, willing and able to embrace the new processes and systems associated with a smart grid. The change management is a complex process. The change should occur at various levels such as system, process, people and organization. Communication is the oil that ensures everything works properly. It is essential to communicate the scope of solar grid and related solar computing to the public policy makers, state and central governments, corporate executives, academic and research community.

The fifth element of the deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. Technology trajectory is the path that the technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. The technology of solar computing is now passing through the emergence phase of S-curve. Initially, it may be difficult and costly to improve the performance of the technology. The performance is expected to improve with better understanding of the fundamental principles and system architecture. The dominant design should consider an optimal set of most advanced technological features which can meet the demand of the consumers in the best possible way. It is really interesting to analyze the impact of various factors on the trajectory of smart solar grid technology.

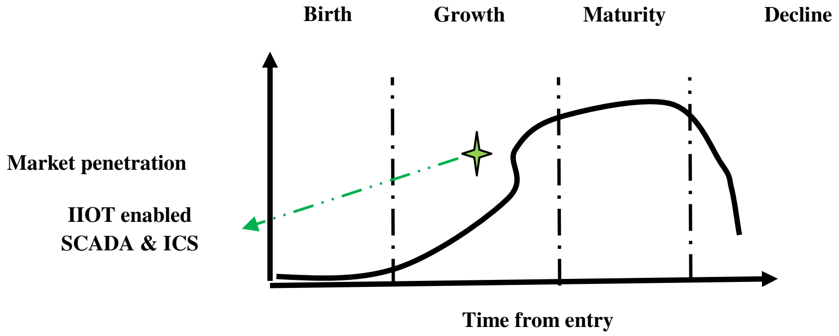


Figure 10.17 : Technology life-cycle analysis of SCADA & ICS

The fifth element of deep analytics is strategy. This element can be analyzed from different dimensions such as R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. Technology trajectory is the path that IIoT enabled ICS and SCADA technology takes through its time and life-cycle from the perspectives of rate of performance improvement, rate of diffusion or rate of adoption in the market. This technology is now passing

through the growth phase of S-curve. Initially, it is difficult and costly to improve the performance of the technology. The performance is expected to improve with better understanding of the fundamental principles and system architecture. The dominant design should consider an optimal set of most advanced technological features which can meet the demand of the customer, supply and design chain in the best possible way. It is really interesting to analyze the impact of various factors on the trajectory IIOT enabled SCADA and ICS technology.

Strategy 1 : SIVM verifies innate and adaptive system immunity in terms of collective, machine, security, collaborative and business intelligence through multi-dimensional view on intelligent reasoning.

SIVM is defined by a set of elements : system, a group of agents, a finite set of inputs, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payment function, an optimal set of moves, revelation principle and model checking or system verification protocol. The proposed mechanism evaluates the innate and adaptive immunity of a system which is defined by a set of states (e.g. initial, goal, local and global) and state transition relations.

The mechanism follows a set of strategic moves. The basic building block of the mechanism is an analytics having multidimensional view of intelligent reasoning. Reasoning has multiple dimensions like common sense, automated theorem proving, planning, understanding, hypothetical, simulation dynamics and envisioning i.e. imagination or anticipation of alternatives. The inference engine selects appropriate reasoning techniques from a list of options such as logical, analytical, case based, forward and backward chaining, sequential, parallel, uncertainty, probabilistic, approximation, predictive, imaginative and perception based reasoning depending on the demand of an application. Another important move is the collection of evidence through private search which may require a balance between breadth and depth optimally.

The critical challenge is how to detect the danger signal from a system? The mechanism evaluates system immunity (i) combinatorially in terms of collective, machine intelligence, security, collaborative and business intelligence. The *collective intelligence* (a) is defined in terms of scope, input, output, process, agents and system dynamics. For a complex application, it verifies coordination and integration among system, strategy, structure, staff, style, skill and shared vision. What is being done by the various components of a system? Who is doing? Why? How? Where? When? The *machine intelligence* (b) checks the system in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy. For example, it should check preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states and state transition plans of the information system associated with ICS/SCADA.

The *security intelligence* (c) verifies the system in terms of authentication, authorization, correct identification, non-repudiation, integrity, audit and privacy; rationality, fairness, correctness, resiliency, adaptation, transparency,

accountability, trust, commitment, reliability and consistency. The *collaborative intelligence* (d) evaluates the feasibility and effectiveness of human-computer interaction to achieve single or multiple set of goals, information sharing principle and negotiation protocol. The *business intelligence* (e) is associated with business rules such as HR policy, payment function, cost sharing, bonus, contractual clauses, quality, performance, productivity, incentive policy and competitive intelligence.

The mechanism verifies system immunity through a set of verification algorithms. It is possible to follow various strategies like model checking, simulation, testing and deductive reasoning for automated verification. Simulation is done on the model while testing is performed on the actual product. It checks the correctness of output for a given input. Deductive reasoning tries to check the correctness of a system using axioms and proof rules. There is risk of state space explosion problem in case of a complex system with many components interacting with one another; it may be hard to evaluate the efficiency of coordination and integration appropriately. Some applications also demand semi-automated and natural verification protocol. The mechanism calls threat analytics and assesses risks of single or multiple attacks on the system under consideration: analyze performance, sensitivity, trends, exception and alerts; checks what is corrupted or compromised: agents, protocol, communication, data, application and computing schema? Performs time series analysis: what occurred? what is occuring? what will occur? assess probability of occurrence and impact; explores insights : how and why did it occur? do cause-effect analysis; recommends : what is the next best action? predicts: what is the best or worst that can happen?

Strategy 2 : SIVM verifies security intelligence collectively through rational threat analytics.

Model checking is an automated technique for verifying a finite state concurrent system such as a hardware or software system. Model checking has three steps: represent a system by automata, represent the property of a system by logic and design model checking algorithm. The security intelligence of SCADA is a multi-dimensional parameter which is defined at five different levels L1,L2,L3,L4 and L5. At level L1, it is essential to verify the security of data schema in terms of authentication, authorization, correct identification, privacy and audit of access control mechanism offered by the system. In this case, the system should ask the identity and authentication of one or more agents involved in SCADA operation and system administration. The agents of the same trust zone may skip authentication but it is essential for all sensitive communication across different trust boundaries. After correct identification and authentication, SIVM should address the issue of authorization. The system should be configured in such a way that an unauthorized agent cannot perform any task out of scope. The system should ask the credentials of the requester; validate the credentials and authorize the agents to perform a specific task as per agreed protocol. Each agent should be assigned an explicit set of access rights according to role. Privacy is another important issue; an agent can view only the information according to authorized access rights. A protocol preserves privacy if no agent learns anything more than its output; the only

information that should be disclosed about other agent's inputs is what can be derived from the output itself. The privacy of data may be preserved in different ways such as adding random noise to data, splitting a message into multiple parts randomly and sending each part to an agent through a number of parties hiding the identity of the source, controlling the sequence of passing selected messages from an agent to others through serial or parallel mode of communication, dynamically modifying the sequence of events and agents through random selection and permuting the sequence of messages randomly. The agents must commit the confidentiality of data exchange associated with private communication.

At level L2, it is essential to verify the computing schema in terms of fairness, correctness, transparency, accountability and trust. A protocol ensures correctness if the sending agent broadcasts correct data free from any false data injection attack and each recipient receives the same correct data in time without any change and modification done by any malicious agent. Fairness is associated with proper resource allocation, trust, commitment, honesty and rational reasoning of the agents involved in SCADA system administration. Fairness ensures that something will or will not occur infinitely often under certain conditions. The mechanism must ensure the accountability and responsibility of the agents in access control, data integrity and non-repudiation. The transparency of SCADA system administration is associated with communication protocols and revelation principle.

At level L3, it is essential to verify the application schema in terms of system performance. The performance of the system and quality of service is expected to be consistent and reliable. Reachability ensures that some particular state or situation can be reached. Safety indicates that under certain conditions, an event never occurs. Liveness ensures that under certain conditions an event will ultimately occur. Deadlock freeness indicates that a system can never be in a state in which no progress is possible; this indicates the correctness of a real-time dynamic system. SCADA is expected to be a resilient system. The resiliency measures the ability to and the speed at which the system can return to normal performance level following a disruption.

At level L4, SIVM verifies networking schema and assesses the threats of internal and external malicious attacks on SCADA & ICS such as cyber attack, rubber hose, sybil, node replication, wormhole, coremelt, forward, blackhole, neighbor, jellyfish and crypto jacking attack. At level L_5, SIVM verifies security schema and assesses the risk of multi-party corruption (e.g. sender, receiver, data, communication channel, mechanism and protocol) and business intelligence of payment function.

Strategy 3 : The security intelligence of an industrial control system is verified comprehensively in terms of correctness of computing schema, stability and robustness in system performance of the plant, data, networking, security and application schema.

Please refer to second test case in the appendix where SIVM is applied for a plant having supervisory adaptive fuzzy control. Let us first explain various types of circuits for intelligent process control of the plant. Next, it is essential to call threat analytics and verify the security intelligence of data, computing, application, networking and security schema at levels 1,2,3,4 and 5. At level L1, it is crucial to verify the data schema in terms of authentication, authorization, correct

identification, privacy, audit, confidentiality, integrity, non-repudiation, locking of passwords, false data injection attack and intrusion for proper access control of the plant. Any flaws in access control may affect the stable performance of the plant negatively. A malicious agent can take over the control of the plant completely or partially by hacking system control passwords or compromising system administration.

Next, let us consider level L2 to verify the computing schema. Fuzzy logic is a multi-valued logic used for approximate reasoning. Fuzzy logic based algorithms are used for the control of complex plants through fuzzy controllers. The fuzzy controllers (FC) operate based on IF-THEN fuzzy rules. Industrial process control systems use various types of controllers such as P/PI/PID through adaptive gain scheduling, supervisory control architectures and algorithms. The fuzzy controllers use IF-THEN rules, can learn universal approximation property and can deal with fuzzy values. If there are flaws in design of these basic features of fuzzy controllers, a plant may face various types of problems in terms of system performance, stability and robustness.

A plant's behavior can be defined by a set of IF-THEN fuzzy rules based on knowledge acquisition from knowledge based expert system, ANN and GA based algorithms. ANN and GA are used to learn fuzzy rules through structural identification which requires structural apriori knowledge such as linear or nonlinear control of a system. Another approach is parameter identification, scaling and normalization of physical signals. Another important feature is universal approximation: a fuzzy system with IF-THEN rules firing, defuzzification and membership function can approximate any real continuous function with certain approximation error due to the overlap of membership function from IF parts of a set of fuzzy rules. The inputs to the fuzzy controller are fuzzy values; they are quantitative numbers being obtained from different sources. For example, the intensity of a signal with respect to time interval is expressed by a membership function. FCs are able to deal with fuzzy value through heuristics or model based approaches.

The objective of fuzzy control is to design a feedback control law in the form of a set of fuzzy rules such that the closed loop system exhibits the desired behavior of a given model of the system and its desired behavior. The quality of nonlinear control is measured in terms of system performance, stability, robustness, accuracy and response speed In case of stabilization, the state vector of a closed loop system should be stabilized around a set point of the state space. Here, the challenge is to define a set of fuzzy rules based control law. In case of tracking, a FC is to be designed so that the output of closed loop system follows a time varying trajectory. The basic objective is to find a control law in terms of a set of fuzzy rules such that the tracking error $[x(t) - x^d(t)]$ tends to zero. In fact, stabilization is a special type of tracking where the desired trajectory is constant.

Next, let us consider system performance of a plant in terms of computing and application schema at level L3. In case of linear control, the behavior of a closed loop system can be specified in exact quantitative terms such as rise time, setting time, overshoot and undershoot. The desired behavior of a non-linear closed system can be specified in qualitative terms such as stability, accuracy, response speed and

robustness. In case of linear control, stability implies the ability to withstand bounded disturbances in linear range of operation of the system. In case of nonlinear control, the behavior of the system is analyzed in terms of effects of positive disturbances and robustness. Robustness is the sensitivity of the closed loop system to various types of effects such as measurement noise, disturbances and unmodelled dynamics. The closed loop system must be insensitive to these effects. Accuracy and response speed must be considered for desired trajectories in the region of operation. Moreover, it is important to verify the plant's performance in terms of reliability, consistency, resiliency, liveness, denial of service (DoS) attack, deadlock freeness, synchronization and application integration. It is expected to minimize human error in plant's operation from the perspectives of correct decision making and adjustment of the setting of plant's parameters.

The verification of correctness of computing schema of a fuzzy controller is a critical issue. A fuzzy logic controller defines a control law in terms of a transfer element due to non-linear nature of computation. The fuzzy control law is expressed by a set of 'IF THEN' fuzzy rules. 'IF' part of a fuzzy rule describes a fuzzy region in the state space. 'THEN' part specifies a control law applicable within fuzzy region from IF part of the same rule. FC yields a smooth non-linear control law through the operation of aggregation and defuzzification. The correctness of computing schema is associated with a set of computational steps such as input scaling or normalization, fuzzification of controller input variables, inference rule firing, defuzzification of controller output variables and output scaling or denormalization.

In case of supervisory control, one or more controllers are supervised by a control law on a higher level. The low level controllers perform a specific task under certain conditions keeping a predefined error between desired state and current state, performing a specific control task and being at a specific location of the state space. Supervision is required only if some of the predefined conditions fail : change the set of control parameters or switches from one control strategy to another. Supervisory algorithms are formulated in terms of IF-THEN rules. Fuzzy IF-THEN rules support soft supervision and avoid hard switching between set of parameters or between control structures.

In case of adaptive control, a dynamic system may have a known structure, but uncertain or slowly varying non-linear parameters. Direct adaptive approaches start with sufficient knowledge about the system structure and its parameters. Direct change of controller parameters optimize the system's behavior with respect to a given criterion. Indirect adaptive control methods estimate the uncertain parameters of the system under control on-line and use the estimated parameters in the computation of the control law. Adaptive control audits system performance in terms of stability, robustness, tracking convergence, tuning and optimization of various parameters like scaling factors for input and output signals, input and output membership functions and fuzzy IF-THEN rules.

It is also essential to audit security intelligence of the networking schema of the plant at level L_4: detect threats of internal and external attacks such as cyber, rubber hose attack, sybil, node replication, wormhole, coremelt, forward, blackhole, neighbor, jellyfish and Crypto jacking attack. A real-time monitoring system must

audit multi-party corruption at level L_5 [e.g. sender, receiver, data, communication channel, mechanism, protocol, process, procedure]. The system administrator should mitigate the risks of various threats through proactive, reactive approaches and sense-and-response against bad luck like the occurrence of natural disaster.

Strategy 4 : SCADA / ICS requires both automated and semi-automated verification mechanisms for intrusion detection.

SCADA / ICS calls threat analytics and a set of model checking algorithms for various phases : exploratory phase for locating errors, fault finding phase through cause effect analysis, diagnostics tool for program model checking and real-time system verification. Model checking is basically the process of automated verification of the properties of the system under consideration. Given a formal model of a system and property specification in some form of computational logic, the task is to validate whether or not the specification is satisfied in the model. If not, the model checker returns a counter example for the system's flawed behavior to support the debugging of the system. Another important aspect is to check whether or not a knowledge based system is consistent or contains anomalies through a set of diagnostics tools.

There are two different phases : explanatory phase to locate errors and fault finding phase to look for short error trails. Model checking is an efficient verification technique for communication protocol validation, embedded system, software programmers', workflow analysis and schedule check. The basic objective of the model checking algorithm is to locate errors in a system efficiently. If an error is found, the model checker produces a counter example how the errors occur for debugging of the system. A counter example may be the execution of the system i.e. a path or tree. A model checker is expected to find out error states efficiently and produce a simple counterexample. There are two primary approaches of model checking: symbolic and explicit state. Symbolic model checking applies a symbolic representation of the state set for property validation. Explicit state approach searches the global state of a system by a transition function. The efficiency of model checking algorithms is measured in terms of automation and error reporting capabilities. The computational intelligence is also associated with the complexity of threat analytics equipped with the features of data visualization and performance measurement.

The threat analytics analyze system performance, sensitivity, trends, exception and alerts along two dimensions: time and insights. The analysis on time dimension may be as follows: what is corrupted or compromised in the system: agents, communication schema, data schema, application schema, computing schema and protocol? what occurred? what is occuring? what will occur? Assess probability of occurrence and impact. The analysis on insights may be as follows : how and why did the threat occur? What is the output of cause-effect analysis? The analytics also recommends what is the next best action? It predicts what is the best or worst that can happen?

How can you assess the immunity of ICS against intrusion in the form of sybil, cloning, wormhole or node capture attacks? **Traditional intrusion detection**

techniques may not be able to sense danger signal or perform negative or clonal selection due to non-availability of intelligent threat analytics and ill-defined system immunity. The verification algorithm is expected to detect, assess and mitigate the risks of intrusion attacks more efficiently as compared to traditional approaches since it has a broad vision and adopts a set of AI moves including multi-dimensional view of intelligent reasoning, private search for evidence by balancing breadth and depth optimally and exploring system immunity combinatorially. Another interesting strategy is the use of a rational threat analytics.

Possible functionalities, constraints like computational and communication complexities and systematic features influence the perception of security and trust of a distributed network. For example, the computational power, memory capacity and energy limitations enforce slightly different approaches to the problems of security and privacy in sensor networks. In an open environment, sensor nodes operate without any supervision; a malicious attacker can capture a node for reconfiguration or extract the private data stored in the node through cryptanalysis. An attacker may be able to deploy multiple physical nodes with same identity through cloning or node replication attack. An adversary may be able to deploy multiple identities of a node to affect the trust and reputation of the system through Sybil attack. The attacker may be able to build an additional communication channel to capture private communication through wormhole attack. A key can be compromised either by physical extraction from a captured node or by breach in SMC protocol. The denial of service attack renders a node by overloading it with unnecessary operations and communication and may be able to make the whole network inoperable. Coremelt attacks can target communication links blocking the exchange of useful information. Replay attacks allows an attacker to record messages at one instance and replay it later at different locations.

There are possibilities of blackhole, jellyfish, neighbor and rushing attacks. A blackhole attacking agent tries to intercept data packets of the multicast session and then drops some or all data packets it receives instead of forwarding the same to the next node of the routing path and results very low packet delivery ratio. A jellyfish attacker intrudes into the multicast forwarding group and delays data packets unnecessarily and results high end-to-end delay and degrades the performance of real-time application. A neighborhood attacking agent forwards a packet without recording its ID in the packet resulting a disrupted route where two nodes believe that they are neighbors though actually they are not. Rushing attack exploits duplicate suppression mechanisms by forwarding route discovery packets very fast.

The proposed algorithm explores the concept of next generation Intrusion Detection System (IDS) based on bio-inspired artificial intelligence and immunological theories. The critical challenge of information security is to determine the difference between normal and malicious activities. Traditionally, a distributed system is protected by access control policy that blocks malicious events. Actually, it should be protected by artificial immune systems through automated and adaptive verification mechanisms based on negative selection i.e. self / non-self discrimination, clonal selection and danger signal detection. Different strategic moves are useful for different situations.

A distributed network consists of a set of entities, a broadcast communication cloud and a set of pipes connecting the entities to the communication cloud. The entities can be partitioned into two subsets: correct and faulty. Each correct entity presents one legitimate identity to other entities of the distributed system. Each faulty entity presents one legitimate identity and one or more counterfeit identities to the other entities. Each identity is an informational abstract representation of an entity that persists across multiple communication events. The entities communicate with each other through messages. A malicious agent may control multiple pseudonymous identities and can manipulate, disrupt or corrupt a distributed computing application that relies on redundancy. This is known as sybil attack. Sybil attacks may affect fair resource allocation, routing mechanisms, voting, aggregation and storage of distributed data by injecting false data or suppressing critical data. A large-scale distributed system is highly vulnerable to Sybil attack; it includes sensor and mobile ad hoc networks, p2p applications and SCADA network.

The basic objective of intrusion detection mechanism is to monitor the actions of the users on distributed network and detect the occurrence of any intrusion. Here the challenge is how to perform negative selection, clonal selection and danger signal detection. Auditing is primarily required to validate the security policies and to review the observed behaviors of distributed applications, users and database. User profiling monitors and analyzes the activities of the users. Data profiling analyzes the managed data. In case of anomaly detection, the data of repetitive and usual behavior of the users is collected and suitably represented as normal profiles. The profile and the activities of the current user is compared with the normal profile. If there is significant mismatch, it indicates an intrusion in the network. It is useful for unknown attack. Misuse detection is useful for known attack. SIVM follows a set of AI moves to detect the risk of intrusion:

(a) *multi-dimensional view of intelligent reasoning* {logical, analytical, case based, forward and backward chaining, probabilistic, predictive, perception based approximation reasoning} for system monitoring;

(b) define system immunity (i) combinatorially. i = f(a_i,b_i,c_i,d_i,e_i); a_i: collective intelligence, b_i: machine intelligence; c_i: security intelligence; d_i: collaborative intelligence; e_i: business intelligence;

(c) *assess system immunity* (S_i) through a hybrid approach in terms of negative selection, danger signal detection, clonal selection and suppression*;*

(d) *verify collective intelligence* in terms of policy, scope, input, output, process, agents, location and system dynamics;

(e) *define collaborative intelligence* (revelation principle);

(f) *evaluate business intelligence in terms of* payment function and incentive;

(g) *monitor machine intelligence* in terms of safety, liveness, concurrency, reachability, deadlock freeness, scalability and accuracy. For an information system, it should check preconditions, post conditions, triggering events, main flow, sub flow, alternate flow, exception flow, computational intelligence, communication cost, traffic congestion, time and space complexity, resources, capacity utilization, load, initial and goal states, local and global states, state transition plans*;*

(h) *check security intelligence in terms of* safety, authentication, authorization, correct identification, non-repudiation, integrity, audit and group, forward and

backward privacy; rationality, fairness, correctness, resiliency, adaptation, transparency, accountability, trust, reliability, consistency, commitment).

- **Recognise pattern of intrusion attack like sybil, cloning or node replication, wormhole and node capture;**
- **Sense possibilities and impact of secondary threats such as coremelt, blackhole, jellyfish, rushing, neighbor, replay and shilling attacks;**
- **Select single or multiple approaches from trusted explicit and implicit certification, robust authentication checking of e-passport, resource testing, auction and incentive based sybil detection game;**
- **Verify efficiency of cryptographic signcryption algorithms for private communication.**

There are various approaches of sybil detection: trusted explicit and implicit certification, robust authentication protocol, resource testing, auction and incentive based sybil detection game. In case of trusted certification, a centralized authority assigns a unique identity to each entity. The centralized authority can verify computing, storage and bandwidth capability of the entities on periodic basis. A local identity (l) accepts the identity (i) of an entity (e) if e presents i successfully to l. An entity may validate the identity of another identity through a trusted agency or other entities or by itself directly. In the absence of a trusted authority, an entity may directly validate the identities of other entities or it may accept identities vouched by other accepted entities. The system must ensure that distinct identities refer to distinct entities. An entity can validate the identity of other entities directly through the verification of communication, storage and computation capabilities. In case of indirect identity validation, an entity may validate a set of identities which have been verified by a sufficient count of other identities that it has already accepted. But, a group of faulty entities can vouch for Sybil identities.

A *wormhole* attacker records packets at one point in adhoc wireless communication network, tunnels the packets possibly selectively to another point and retransmits them there into the network. The attacker may not compromise any hosts and even if all communication protocols provide authenticity and confidentiality correctly. *Packet leashes* may be used for detecting and defending against wormhole attacks. A leash is any information that is attached with a packet to restrict its maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sending agent. A temporal leash ensures that the packet has an upper bound on its lifetime which restricts the maximum travel distance.

Sensor node attestation verification is an intelligent move to detect intrusion : check if a sensor node is tampered by an adversary; check the configuration and correct setting of each sensor node; detect whether malicious software is loaded into sensor nodes; verify the integrity of the code; perform secure code updates and ensure untampered execution of code. Each node should be attested with a valid digital test certificate. The verification algorithm must verify the identity and tampering status of each node. The basic objective of device attestation is that a malicious agent should not be able to configure or change correct setting of each node. A challenge response protocol is employed between a trusted external verifier and a sensor node.

Each sensor node should be is provided with an 'e-passport' which should have unique identification features like biometric traits. It is an open issue of research: can a sensor node be equipped with traits like unique biometric features of a human being (e.g. voice, fingerprints, retina, vein patterns and facial dimensions)? An e-passport should have unique passport identification number, time stamp (or date of birth), erection testing and commissioning history, location, digital signature of issuing authority and neighborhood data. It is essential to check the authenticity of e-passport data of each sensor node periodically or for specific suspicious cases to detect intrusion. A single move may not be sufficient to detect intrusion.

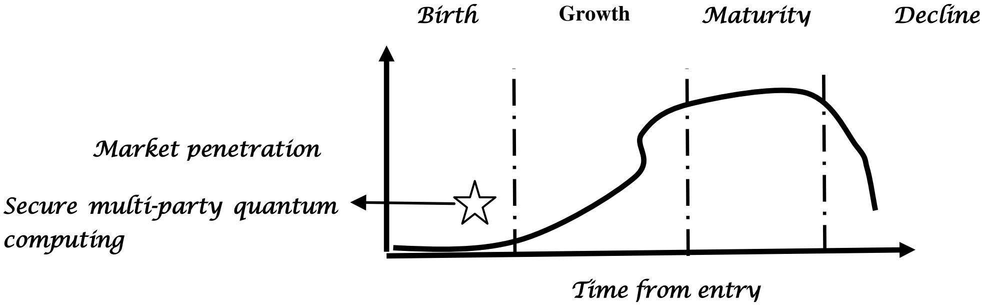


Figure 10.18 : Technology life–cycle analysis of secure quantum computing

The next issue is to analyze the strategy for secure multi-party quantum computing in terms of R&D policy, learning curve, SWOT analysis, technology life-cycle analysis and knowledge management strategy. An intelligent R&D policy should be defined in terms of shared vision, goal, strategic alliance, collaborative, collective and business intelligence. Top technological innovations are closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of quantum computing and computers today. Diffusion is the movement of molecules from high density zone to low density zone of a solution. Can an emerging technology like quantum computing diffuse in the same way globally? What is the pressure acting on technology diffusion? Is the external pressure natural or artificial? It is rational to evaluate strength, weakness, opportunities and threats of quaqtum computing as compared to traditional procedure. Strength indicates positive aspects, benefits and advantages of a strategic option : quantum computing is expected to improve the speed of traditional computing. Weakness indicates negative aspects, limitations and disadvantages of that option. Is the cost of computation and communication high as compared to traditional computing method? Opportunities indicate the areas of growth of market and industries from the perspective of profit; it is possible to develop super computers based on quantum computing. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses : existing technology of computer manufacturing may face threats of substitutes in future. Another important issue is technology life-cycle analysis of secure multi-party quantum computing.. Existing comput manufacturing

technology is expected to be phased out with the evolution of secure multiparty quantum computing; which is presently at the emergence phase of S-curve.

The power of quantum computation is another critical issue. How powerful are quantum computers? What gives them their power? Nobody knows it precisely, Quantum computers are expected to be more powerful than classical computers. Based on computational complexity theory, a particular set of problems are expected to be solved efficiently on a quantum computer, where a bounded probability of error is allowed. Classical computers have difficulty simulating general quantum systems since the number of complex numbers needed to describe a quantum system generally grows exponentially with the size of the system rather than linearly,

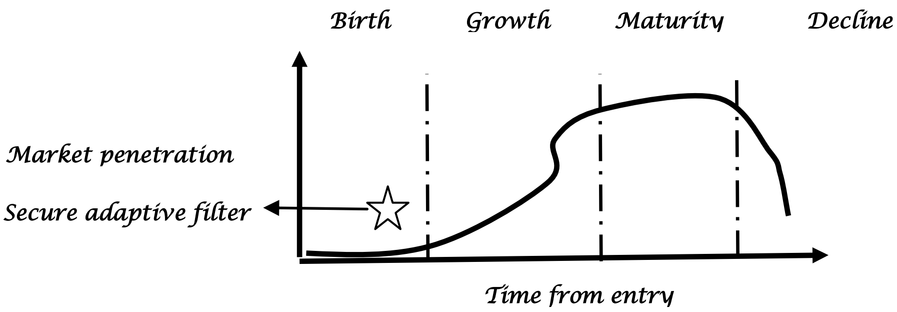


Figure 10.19 : Technology life–cycle analysis of secure adaptive filter

Let us explore the strategy of innovation on secure adaptive filter in terms of SWOT analysis and technology life-cycle analysis. Intelligent Top technological innovations are closely associated with various strategies of organization learning and knowledge management, more specifically creation, storage, transfer and intelligent application of knowledge. It is essential to analyze strength, weakness, opportunities, threats, technological trajectories, technology diffusion and dominant design of secure adaptive filter today. It is rational to evaluate strength, weakness, opportunities and threats of Cuckoo filter with Bloom filter. Strength indicates positive aspects, benefits and advantages of the filter: Weakness indicates negative aspects, limitations and disadvantages of that option. Is the cost of computation and communication of cuckoo filter high as compared to bloom filter? Opportunities indicate the areas of growth of market and industries from the perspective of profit; it is possible to develop secure adaptive filter for modern communication networking and database applications. Threats are the risks or challenges posed by an unfavorable trend causing deterioration of profit or revenue and losses : existing technology of adative filter may face threats of various types of malicious attacks in future.

Another important issue is technology life-cycle analysis of secure adaptive filter. No element in this universe exists eternally. Similarly, each technology emerges, grows to some level of maturity and then declines and eventually expires. It is essential to evaluate the status of each technological innovation through TLC analysis. Some technologies may have relatively long technology life-cycle; others never reach a

maturity stage. Emergence of new technologies follows a complex nonlinear process. It is hard to understand how the technology life-cycle interacts with other technologies, systems, cultures, enterprise activities and impacts on society. All technologies evolve from their parents at birth or emergence phase; they interact with each other to form complex technological ecologies. The parents add their technological DNA which interacts to form the new development. A new technological development must be nurtured; many technologies perish before they are embedded in their environments. Next phase is growth; if a technology survives its early phases, it adapts and forwards to its intended environment with the emergence of competitors. This is a question of struggle for existence and survival for the fittest. Next phase is a stable maturity state with a set of incremental changes. At some point, all technologies reach a point of unstable maturity i.e. a strategic inflection point. The final stage is decline and phase out or expire; all technologies eventually decline and are phased out or expire at a substantial cost. Existing technology of Bloom filter is expected to be phased out with the evolution of Cuckoo filter. The technology of secure adaptive filter is presently at the emergence phase of S-curve.

6. STAFF-RESOURCES

Staff-resources Analytics

Emerging digital technologies demand efficient staff-resources which should be analyzed in terms of sources of innovation and roles of academic institutes, computer science and information technology engineers, government and collaborative networks and optimal utilization of critical resources. The innovation demands the commitment of creative experts in IT and computer science who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab and academic institutions of state and central government. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision in various domains such as requirements engineering, system design, coding, testing and performance optimization. The critical resources are intelligent hardware, software, security and networking solutions.

Innovation demands the commitment of creative people. Creativity is the underlying process for technological innovation which promotes new ideas through intellectual abilities, thinking style, knowledge, personality, motivation, commitment and interaction with environment. Individual inventors may contribute through their inventive and entrepreneurial traits, skills and knowledge in multiple domains and highly curious argumentative mindset. Some users or customers or clients or private nonprofit organizations may innovate new products or services based on their own needs. Many firms set up excellent R&D lab and also collaborative networks with customers, suppliers, academic institutes, competitors, government laboratories and nonprofit organizations. Many universities define sound research mission and vision

and contribute through publication of research papers. Government also plays an active role in R&D either directly or indirectly or through collaboration networks and start-ups (e.g. science parks and incubators). A complex technological innovation often needs collaborative intelligence to manage the gap between demand and supply of a specific set of capabilities, skills and resources. It is possible to control cost, speed and competencies of technological innovations through efficient sharing mechanisms. It is rational to share the cost and risks of new innovations through creation, storage, transfer and application of knowledge among the partners of the innovation ecosystem.

The expert panel are analyzing the need of staff-resources in terms of sources of innovation and roles of electrical and electronics engineering, information technology, SCADA, industrial control system, power grid, government and collaborative networks and optimal utilization of resources. The innovation demands the commitment of creative experts who can contribute significantly through their intellectual abilities, thinking style, knowledge, motivation and group dynamics. In this connection, collaborative networks are interesting options which should coordinate and integrate the needs and activities of R&D lab, academic institutions, power grids of state and central government, users and supply chain partners effectively. The creative talent should look at the hard problems in unconventional ways, generate new ideas and articulate shared vision.

Traditional scope and approaches of smart grid, ICS and SCADA operations focus on long-term planning and stability to mitigate various types of risks. But, complex operation management requires a mix of traditional and agile approaches to cope with uncertainties. The intension driven role develops collaboration. The event driven role integrates planning and review with learning. The other important roles of the system administrators are to prevent major disruptions and maintaining forward momentum continuously. They must acknowledge the emergence of a problem and then try to minimize the frequency and negative impact of unexpected events in a dynamic environment. They must be people oriented, information information oriented and action oriented.

Mr. Aziz is explaining the need of 5M (man, machine, material, method and money) for the innovation of secure multi-party quantum computing and secure adaptive fllter. In this connection, human capital should be considered as a strategic asset and a sustainable resource of technological innovation. The innovation demands skills of human resources for the innovation of emerging technologies and strategic alignment. Man analyzes various aspects of human capital management of technological innovations such as talent acquisition and retention strategy, training, and performance evaluation. 'Machine' analyzes the basic aspects of quantum computers and secure adaptive filters; material analyzes the demand of essential components of quantum computers. Method explores various aspects of process innovation, intelligent mechanism and procedure for the innovation on secure quantum computing and filter. Finally, money highlights optimal fund allocation for the innovation on quantum computing and secure adaptive filter.

7. SKILL-STYLE-SUPPORT

Skill-style-support Analytics

Prof. Pearson thinks that the workforce involved in digital innovations are expected to develop different types of skills in technical (Computer science, Information technology, MIS), research and development, knowledge management, system design and project management. It is essential to teach the aforesaid technologies in various programmes of computer science, BCA, MCA, Electrical and Electronics engineering, information and communication technology as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented. The emerging digital technologies also demand efficient leadership style in terms of optimal resource allocation and utilization, collaboration, coordination and communication.

Next, let us focus on support. The emerging digital technologies should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated HR workforce. Active involvement, knowledge sharing and optimal human talent utilization is essential for the diffusion of new technology. New skill should be developed in digital, information and communication technologies. The business model requires the support of a good human resource management system for talent acquisition, talent retention, skill development, training, career growth planning, incentive, reward, recognition and payment function. The workforce should develop different types of skills such as research and development, system design, project management, testing, commissioning and system maintenance. The system administrators must have leadership skill in terms of smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes.

What should be the innovation model for emerging digital technology? Is it possible to adopt K-A-B-C-D-E-T-F model? Knowledge managers should arrange various types of events such as workshops, seminars and conferences so that the innovators can acquire the basic and fundamental concept. The activators should initiate the innovation process by identifying a set of good research problems through scope analysis. Random selection of research problem should be avoided by evaluating the strength, experience and skill of the innovators. The research problem should have potential business intelligence and social benefits. The browsers should search for information; investigate throughout the process and find relevant data or

information to start innovation. The creators should analyze the gap and think of to-be system; generate new ideas, concepts and possibilities and search for new solutions. The developers should transform the ideas of the creation phase into good solutions; turn the ideas into deliverables, products and services. They should collaborate with different research forums, industries and experts during this phase. The executors should implement and execute the roadmap of the innovation. The testers should do various types of experiments and laboratory works; verify system dynamics and monitor the performance of the deliverables. Advanced research laboratories are required for complicated testing and experiments. The facilitators should define project plan, corporate governance policy, marketing plan, production plan, investment plan and cost-benefit analysis. They should be able to identify the revenue and profit making stream and fair, rational business intelligence. The government should provide financial assistance to the innovators in patent registration.

The expert panel are discussing on skill-style-support for the innovation of solar computing,, IIOT, SCADA and ICS; they are expected to develop different types of skills in technical (e.g. smart grid, solar computing), research and development, knowledge management, system design and project management. It is essential to teach smart grid technology in various programmes of Electrical and Electronics engineering and information and communication technology as part of graduation, post graduation and Doctoral programmes. The learning community should be involved in consulting, projects and research assignments. They need good resources such as books, journals, software and experimental set up. However, they should understand the motivation of the problems and various issues of technology management through deep analytics. The workforce can develop skills through effective knowledge management programmes and resources which support creation, storage, sharing and application of knowledge. The diffusion of technology requires the support of intelligent leadership style; the leaders must be able to tackle the complexity, pace and novelty of R&D projects through efficient project management, organization structure development, knowledge management and collaborative and cooperative work culture. The leaders are expected to be people, information and action oriented. Smart grid technology demands efficient leadership style in terms of optimal resource allocation and utilization, collaboration, coordination and communication.

It is essential to focus on cause-effects analysis of various unwanted occurrences which may affect individuals, system, organization, critical infrastructure, services, environment or the society. It may be possible that the design of old power grid had not considered the issues of information and cyber security and secure and robust protocols correctly due to specialized hardware and technical skill, proprietary code, protocol standards and operation in closed environment. But, today, the system may be connected to the internet directly or indirectly and controlled by human machine interface. There are other organizational factors such as lack of understanding of the cyber security at the levels of executives and chief information security officers, accountability, lack of proper training and ICT security standards and cultural difference between IT and power grid departments. The primary focus of the power grid department may be efficiency and safety of operation and process

control and less focus on IT and cyber security. Further, there are threats from the perspectives of system architecture, old technology, system design, operation, maintenance and inefficient protocols.

Next, let us focus on support. The system is expected to be resilient. The resiliency measures the ability to and the speed at which it can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of the power grid to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The system administrator must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in grid operation? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs?

The smart grid should be operated by a pool of intelligent, educated, efficient, productive, committed and motivated HR workforce. Active involvement, knowledge sharing and optimal human talent utilization is essential for the diffusion of the new technology related to smart grid. New skill should be developed in erection, testing, commissioning, operations, maintenance and trading of smart power grid. The business model requires the support of a good human resource management system for talent acquisition, talent retention, skill development, training, career growth planning, incentive, reward, recognition and payment function. The workforce should develop different types of skills such as research and development, system design, project management, erection, testing, commissioning and service maintenance. The system administrators must have leadership skill in terms of smart thinking, communication, coordination and change management. The workforce can develop skills through effective knowledge management programmes.

ICS / SCADA operation demands efficient leadership style in terms of optimal resource (5M : man, machine, materials, method, money) allocation and utilization, collaboration and coordination, communication, project management and predictive analytics for analytical and logical reasoning; a set of specific skill set in system administration, technology management, operations management, ERP, SCM, strategic and financial management. It is essential to consider various organizational and human factors such as user awareness of IT and cyber security and overall ICS / SCADA security, transparency in operation and maintenance policies and procedures, threats from disgruntled employees and hackers, weak password protection (e.g. password strength and expiration time), malware protection and external threats in ICS environment (e.g. unauthorized access of ICS / SCADA components).

It is essential to focus on cause-effects analysis of various unwanted occurrences which may affect individuals, system, organization, critical infrastructure, services, environment or the society. It may be possible that the design of old ICS / SCADA technology had not considered the issues of information and cyber security and secure and robust ICS protocols correctly due to specialized hardware and technical skill, proprietary code, protocol standards and operation in closed environment. But, today the system may be connected to the internet directly or

indirectly and controlled by HMI interface. There are other organizational factors such as lack of understanding of the cyber security at the levels of executives and chief information security officers, accountability, lack of proper training and ICT security standards and cultural difference between IT and ICS departments. The primary focus of ICS department may be efficiency and safety of operation and process control and less focus on IT and cyber security. Further, there are threats from the perspectives of system architecture, old technology, system design, operation and maintenance and inefficient protocols.

Next, let us focus on support. The system is expected to be *resilient*. Resiliency measures the ability to and the speed at which it can return to normal performance level following a disruption. Real-time security management involves high cost of computation and communication. The vulnerability of ICS to a disruptive event should be viewed as a combination of likelihood of a disruption and its potential severity. The system administrator must do two critical tasks: assess risks and mitigate the assessed risks. To assess risks, the system administrator should explore basic security intelligence: what can go wrong in ICS operation? what is the probability of the disruption? how severe it will be? what are the consequences if the disruption occurs? A system vulnerability map can be modeled through a set of expected risk metrics, probability of disruptive event and the magnitude of consequences. For example, the map may have four quadrants in a two dimensional space; the vertical axis represents the probability of disruptive event and the horizontal axis represents the magnitude of the consequences.

The system administrator faces a set of challenges to solve the problem of resiliency: what are the critical issues to be focused on? what can be done to reduce the probability of a disruption? what can be done to reduce the impact of a disruption? How to improve the resiliency of the system? The critical steps of risk assessment are to identify a set of feasible risk metrics; assess the probability of each risk metric; assess severity of each risk metric and plot each risk metric in system vulnerability map. The critical steps of risk mitigation are to prioritize risks; do causal analysis for each risk metric; develop specific strategies for each cell of vulnerability map and be adaptive and do real-time system monitoring.

SCADA is a good solution of resilient, smart and intelligent energy grid. An operationally secure power system is one with low probability of system black out or collapse. If the process of cascading failures continues, the system as a whole or its major parts may completely collapse. It is known as system blackout. This problem can be solved through security constrained power system optimization: system monitoring, contingency analysis and corrective action analysis. The contingency analysis is basically computerized simulation technique: it checks line flow limit violation and bus voltage limit violation by simulating each unit and line outage of the power system model. If it finds any violation, it gives alarm. The blackout problem is related to transient stability; it can be solved by fast short circuit clearing, powerful excitation systems and stability control techniques. Voltage stability is another reason of power system collapse. It is concerned with the ability of a power system to maintain acceptable voltages at all buses in the system under normal conditions and after being subjected to a disturbance. Inadequate reactive power support from generators and transmission lines leads to voltage instability or

voltage collapse. Voltage collapse leads to unacceptable voltage instability in a specific zone. This risk can be mitigated by raising generator voltage, generator transformer tap value, reactive compensation by using shunt capacitors, static VAR system and synchronous condensers, OLTC adjustment and strategic load shedding. ***Disaster management plan*** **for a resilient SCADA system is concerned with miscellaneous issues - a set of coordination mechanisms and intelligent priority based resource allocation strategies, organizing disaster management task force during disruption, assessing the expected vulnerabilities approximately, reducing the likelihood of disruptions, collaborative planning for security, building in redundancies i.e. alternative stand-by or back-up system, designing a resilient system and rational investment in training and corporate culture. The SCADA system administrator should develop a business continuity plan for resilience. Collaboration is a strategic tool for developing comprehensive standards of security and safety measures for SCADA system. This is an initiative among all the stakeholders of SCADA system in order to improve the security standards through jointly managed planning, process and shared information.**

A special well-trained taskforce should be ready for disaster management during disruption of SCADA system. The first challenge is to detect the root cause of disruption quickly and recognize. The system administrator should isolate the abnormal process or system components from the normal one. Security and safety measures should be layered. Properly layered security measures woven together can reduce the probability of disruption of a complex system where a single security move may not be adequate to provide adequate security. During disruption, a SCADA system may be isolated from the power grid through a set of protection relays. In fact, a system requires preventive maintenance on periodic basis. The maintenance plan and shut down schedule should be published to the public in advance. In case of transient disaster, the public should be alerted in time to avoid the sudden uncertainties. In manufacturing domain, a steel / cement / automotive plant should be shut down for periodic maintenance or production capacity control adaptively; soft start is essential for intentional disruption of continuous production system.

The SCADA system administrator should identify all connections to SCADA network; disconnect unnecessary connections; evaluate and strengthen the security of any remaining connections to the SCADA network; avoid unnecessary services; should not only rely on traditional security protocols; select appropriate vendors and consultants and implement the optimal set of security features; establish strong controls over any medium that is used as a backdoor into the SCADA network; implement intruder detection system; perform technical audits of SCADA network and the associated applications and should conduct physical surveys of all the remote sites connected with SCADA network regularly. The system administrator should identify and evaluate possible attack scenarios; define the role of security and disaster management workforce clearly; document the IT architecture of the security system of SCADA network; define a risk assessment and risk mitigation strategy; determine the basic security requirement of SCADA system; establish effective configuration management process; conduct self-assessments and establish system back-up and disaster recovery plan. Security workforce plays an important

role to control various types of chaotic situation near SCADA system. Finally, the security reengineering team of SCADA system requires the commitment and support of the leaders and senior management for proper communication of the security policy (e.g. access control, information disclosure), user training and implementation of SCADA security system. Much of the current SCADA system is outdated, unreliable and insecure having high maintenance cost. New capabilities can enhance efficiency and reliability but also create various types of vulnerabilities. The reengineering of SCADA system should focus on distributed computational intelligence, broadband communication capabilities and robust security infrastructure.

Let us explore skill-style-support necessary for the innovation of secure multi-party quantum computing. The workforce involved in innovation of quantum compouting are expected to develop different types of skills in Physics, Computer Science, research and development and knowledge management. The next issue is skill-style-support necessary for the innovation of secure adaptive filter. The workforce involved in innovation of secure adaptive filter are expected to develop different types of skills in Computer Science (e.g. Data Structure, Secure Multi-party Computation), communication technology, research and development and knowledge management. The diffusion of the new technological innovation depends on the skills and capabilities of new start ups and research laboratories globally. The system administrators must have leadership skills in smart thinking, communication, coordination and change management. The workforce should develop skills through effective knowledge management programmes. An effective knowledge management system should support creation, storage, sharing and application of knowledge in a transparent, collaborative and innovative way. The diffusion of secure multi-party quantum computing technology needs the support of great leadership style; The style is basically the quality of leadership; great leaders must have passion, motivation, commitment, support, coordination, integration and excellent communication skill. What should be the innovation model for effective diffusion of quantum computing technology? Is it possible to adopt K-A-B-C-D-E-T-F model?

8. CONCLUSION

It is an interesting option to extend this study from different perspectives : green information system, computation of MPPT based on AI, construction of quantitative models foe self healing mechanism and real-time fault diagnostics. A solar computing system must ensure real-time secure monitoring and sense-and-respond modeling; the system should be able to tune itself automatically to an optimal state adaptively. It should be able to anticipate various types of threats automatically that could disturb the stability of the system. Another important task is to isolate the healthy part from the faulty one. A smart power grid is vulnerable to both natural disasters and intentional attacks, physical and cyber challenges and threats of deception. The size and complexity of the grid structure and related cost of erection, testing, commissioning and maintenance are the major constraints to protect the entire infrastructure physically. There are also threats of act of terrorism on the

disruption of smart grid and related adverse effects on national security, economy and the quality of life of the common people. Energy security demands fundamental rethinking and radical redesign of the existing power grids globally.
Intelligent business and technical analysis of IIOT, ICS and SCADA requires the availability of critical up-to-data, analytical models and tools for rational, fair and correct evaluation of technology innovation. This study can be extended in various ways. It is interesting to extend the scope of the aforesaid system in various emerging applications such as banking and financial services, defense and e-governance. ICS & SCADA networks are potentially vulnerable to intrusion and various types of malicious cyber attacks which may affect the safety of common people and the performance of critical infrastructure seriously and may cause huge financial loss. It is expected to be a resilient system. This work finds a set of interesting research agenda for future works: how to develop intelligent threat analytics and secure verification algorithms from the perspectives of method, target, identity and protocol to ensure confidentiality, authentication, integrity, availability, accountability and access control of ICS and SCADA infrastructure? how to quantify various parameters of security intelligence? Is it possible to develop automated verification and model checking algorithms for ICS and SCADA? We need a new broad outlook, imagination and dreams to solve a complex problem through a set of simple mechanisms.

The expert panel are highlighting some common SMC tools, it is an interesting option to explore how to construct these tools in the setting of Quantum Computing?
***Oblivious transfer*: Oblivious transfer (OT) is a bi-party protocol wherein a receiver learns some information regarding the input of the sender such that the sender does not know what the receiver has learnt. The notion of oblivious transfer has several versions. Rabin introduced the concept of oblivious transfer. In the original OT problem, the receiver learns the secret of the sender with probability ½. 1-out-of-2 oblivious transfer ($OT^1{}_2$) is a protocol by which a sender (S) transfers ignorantly to a receiver (R) one out of two secret messages (Even, Goldreich and Lempel, 1985). 1-out-of-n oblivious transfer is a protocol between two parties. Here, Alice holds n inputs in a particular sequence which is known only to Bob.. At the end of the protocol, Bob learns only 1 out of n inputs and Alice will not know which input Bob has learnt (Naor and Pinkas, 1999). k-out-of-n oblivious transfer protocol is an extended version of 1-out-of-n oblivious transfer where 1≤k≤n-1. Distributed oblivious transfer protocol distributes the task of Alice between several servers and each server holds partial information about the secret (Naor and Pinkas, 2000). The receiver has to contact t (t≥1) or more servers to get the secret otherwise it cannot get any information about the secret. Security is ensured as long as a limited number of servers collude. Oblivious polynomial evaluation is a protocol involving two parties, Alice holding input a polynomial P and Bob with input x. At the end of the protocol, Bob learns P(x) but Alice learns nothing about x. Naor and Pinkas (1999) studied an oblivious evaluation of polynomial problem based on oblivious transfer protocol. Oblivious transfer is a fundamental primitive for cryptography and secure distributed computation and has many applications.**

***Secure function evaluation*:** **Alice with an input x and Bob with an input y want to evaluate a function z = f(x,y) based on their joint inputs in such a way that does not allow any party to gain more information than that is implied by its inputs and the function value. Alice and Bob can achieve this through a protocol known as secure function evaluation. In the field of secure function evaluation, f is represented in various ways - garbled circuit construction), combinatorial circuit, algebraic, as a product of matrices over a large field; low degree polynomial and randomizing polynomials.**

Mixnet **: A mixnet consists of multiple independent mix-servers and it enables a group of senders to send their messages anonymously. Chaum (1988) introduced the concept of mixnet. Later, several researchers proposed mixnet protocols for the shuffling of encrypted messages. The concept of mixnet has been widely applied to design efficient electronic voting schemes. In this case, each voter sends his encrypted ballot to a mixnet. The Mixnet shuffles the posted ballots such that the voter-vote relationship is lost. After the mixing process, multiple tally servers jointly decrypt the encrypted ballot and count the votes. Mixnet can be classified into verifiable mixnet and optimistic mixnet on the basis of correctness proof. Each server of verifiable mixnet provides the proof that its shuffling is correct. On the other side, optimistic mixnet does not provide the verification of correct shuffling by each server. The correctness of the shuffling of the whole mixnet is verified after it generates the output.**

Private comparison **: Yao's millionaire problem is to find out who is richer between two parties such that no information about one party's value is revealed to the other party. Yao first proposed a protocol for this problem without using any untrusted third party. The cost of the protocol was exponential in both time and space. Later, scrambled circuits has been used to solve this problem at linear cost of computation and communication. Cachin (1999) suggested an efficient solution using an oblivious third party. Fishchlin (2001) used the Goldwasser-Micali (GM) encryption scheme to construct a two round non-interactive crypto-computing GT (greater than) protocol. Two inputs can be compared by verifying the most significant bit in which they are different. Similar bits do not affect the result and the effect of unequal low order bits is overshadowed by the high order bits. Based on this principle, Ioannidis and Grama (2003) proposed a private comparison protocol using oblivious transfer scheme. Schoenmaker and Tuyls (2004) used threshold homomorphic encryption scheme to solve private comparison problem. Blake and Kolesnikov (2004) used the concepts of Q-conditional oblivious transfer and the additive homomorphic Paillier cryptosystem to construct a two round private comparison protocol. The computation cost is O(nlogN) where n is the length of the inputs and N is the size of the plaintext domain of Paillier scheme.**

In this session, the panel have analyzed the complexity of emerging technology of secure multi-party quantum computing by reviewing various related works [1-15] - what are the fundamental concepts of quantum computation and quantum

information? what are the scopes of application of SMQC? How to develop these concepts? how to develop quantum errors correctling codes and fault tolerant quantum computation? how to develop cryptographic protocols, private and public key cryptosystems in the setting of SMQC? Wht is the future of SMQC? What can quantum computation and quantum information offer to science, technology and humanity? What are the benefits of SMQC upon omputer science, information theory and Physics? What are the key open problems of quantum computation and quantum information? SMQC is the basic building block to think physically about computation and it yields many new exciting capabilities for information processing and communication. Secure multi-party quantum computation offer hard challenges in terms of computation and communication complexity.

This session shows the application of cryptographically secure protocols for kernelized Support Vector Machines of secure adaptive filter.However, there are still many open problems in private SVM classification, learning and secure adaptive filters. An interesting question is how to compute and securely hide the convergence speed of the private SVM algorithms? Are there any iterative private linear classification methods that need no circuit evaluation. Another relevant issue is private computation of encrypted kernel matrices for structured data. A protocol preserves privacy if no agent learns anything more than its output; the only information that should be disclosed about other agent's inputs is what can be derived from the output itself. Secure multi-party computation preserves privacy of data in different ways; is it possible to apply SMC protocols for secure adaptive filter? What are the algorithms? is the cost of computation and communication high in secure multi-party computation of an adaptive filter? Privacy is one of the primary concerns of secure adaptive filter; is it possible to address the issue utilizing the concept of cryptography and secure multiparty computation? The fundamental objectives of cryptography are to provide confidentiality, data integrity, authentication and non-repudiation. Cryptography ensures privacy and secrecy of information through encryption and decryption methods. The challenge is how to apply existing encryption and decryption algorithms in secure adaptive filter : is it possible to perform quantitative operations of secure adaptive filter on encrypted data? How? Is it possible to apply *digital signature* for secure adaptive filter? how to apply existing digital signature algorithms in secure adaptive filter : is it possible to perform quantitative operations of secure adaptive filter on digitally signed data? How? Is it possible to apply *signcryption* for secure adaptive filter? how to apply existing signcryption and unsigncryption algorithms for secure adaptive filter : is it possible to perform private search on signcrypted data? How?

The central message of this summit is that the success of technology innovation projects depends on several factors: strength, weakness, opportunities, threats, technology life-cycle, understanding the needs of consumers, competitive environment, blind spots and the ability to recognize and align the partners associated with the value chain and innovation ecosystem. Deep analytics is essential to coordinate, integrate and synchronize '7-S' elements: scope, system, structure, staff-resources, skill-style-support, security and strategy. Even the most brilliant

innovation cannot succeed when its value creation depends on innovation of other technologies. This book evaluates a set of emerging technologies for humanity; most of these technology innovations are at emergence stage, some others are at growth stage. Hopefully, deep analytics should be able to accelerate the pace of these emerging technological innovations. Let us discuss the limitations and future scope of this summit. In fact, the aforesaid content is the summary of the discussions during various sessions of the summit and are focused on emerging technologies associated with electrical and electronics engineering, information and communication technologies and computer science. There are other various branches of science and technology such as Mathematics, Physics, Chemistry, Biology, Earth science, Geology, mechanical, chemical, petrochemicals, oil and gas, pharmacy, biotechnology, genetics, metallurgical, civil, structural, construction, production and power plant engineering. It is essential to have depth and breadth of knowledge to explore emerging technologies in those branches of engineering. Secondly, deep analytics demand the support of quality technical and business data and efficient quantitative tools and techniques to evaluate the potential of a technology, to perform technology life-cycle analysis, technology diffusion, adoption, infusion and innovation, dominant design, blind spots and spillover effects. It is also essential to evaluate these emerging technologies deeply from the perspective of numerical, statistical, quantitative and qualitative analysis based on up-to-date data. In fact, there is no end of this intelligent deep analysis. There is no end of the debate on the strength, weakness, threats and opportunities of emerging technologies and comparison with existing technologies. ***Let us try to save the world.....***

FURTHER READING

- **Armburst, M. et al. (2010). A view of cloud computing, Communications of the ACM, 53(4), 50-58.**
- **Buyya, R., Yeo, C.S., Venugopal, S., Broberg,J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility. Future generation computer systems.**
- **Chakraborty, S. (2007). A study of several privacy-preserving multi-party negotiation problems with applications to supply chain management. Fellow programme dissertation, Indian Institute of Management Calcutta.**
- **Forouzan, B.A. (2007). Cryptography & network security. McGraw Hill.**
- **Furht,B. and Escalante, A. (2010). Handbook of Cloud Computing. Springer.**
- **Goldreich, O. (2004). Foundations of Cryptography, Basic Applications. Volume 2. Cambridge University Press.**
- **Reports of Gartner and Forrester; 2017,2018,2019.**
- **Beloglazov, A., Buyya, R., Lee, Y.C and Zomaya, A. (2011). A taxonomy and survey of energy efficient data centers and cloud computing systems. Advances in computers, volume 82.**
- **Wang (2012). "Enterprise cloud service architectures". Information Technology and Management. 13 (4): 445–454. doi:10.1007/s10799-012-0139-4.**

- "What is Cloud Computing?". Amazon Web Services. 2013-03-19. Retrieved 2013-03-20.
- Ted Simpson, Jason Novak, Hands on Virtual Computing, 2017, ISBN 1337515744, p. 451
- Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld.
- Kumar, Guddu (9 September 2019). "A Review on Data Protection of Cloud Computing Security, Benefits, Risks and Suggestions" (PDF). United International Journal for Research & Technology. 1 (2): 26. Retrieved 9 September2019.
- Antonio Regalado (31 October 2011). "Who Coined 'Cloud Computing'?". Technology Review. MIT.
- Griffin, Ry'mone (2018-11-20). Internet Governance. Scientific e-Resources. ISBN 978-1-83947-395-1.
- "Distributed Application Architecture". Sun Microsystem.
- Bruneo, Dario; Distefano, Salvatore; Longo, Francesco; Puliafito, Antonio; Scarpa, Marco (2013). "Workload-Based Software Rejuvenation in Cloud Systems". IEEE Transactions on Computers. 62 (6): 1072–1085. doi:10.1109/TC.2013.30.
- Kuperberg, Michael; Herbst, Nikolas; Kistowski, Joakim Von; Reussner, Ralf (2011). "Defining and Measuring Cloud Elasticity". KIT Software Quality Departement. doi:10.5445/IR/1000023476.
- Marston, Sean; Li, Zhi; Bandyopadhyay, Subhajyoti; Zhang, Juheng; Ghalsasi, Anand (2011-04-01). "Cloud computing – The business perspective". Decision Support Systems. 51(1): 176–189. doi:10.1016/j.dss.2010.12.006.
- Mills, Elinor (2009-01-27). "Cloud computing security forecast: Clear skies". CNET News.
- Boniface, M.; et al. (2010). Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds. 5th International Conference on Internet and Web Applications and Services (ICIW). Barcelona, Spain: IEEE. pp. 155–160. doi:10.1109/ICIW.2010.91.
- Butler, Brandon (2017-10-17). "What is hybrid cloud computing? The benefits of mixing private and public cloud services". Network World.
- "Business Intelligence Takes to Cloud for Small Businesses". CIO.com. 2014-06-04.
- Haghighat, Mohammad; Zonouz, Saman; Abdel-Mottaleb, Mohamed (2015). "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification". Expert Systems with Applications. 42 (21): 7905–7916. doi:10.1016/j.eswa.2015.06.025.
- Ray, Neville (June 18, 2018). "FCC testimony Neville Ray". FCC.gov
- "Preparing the ground for IMT-2020". www.3gpp.org. Archived from the original on April 14, 2019.
- Rappaport, T.S.; Sun, Shu; Mayzus, R.; Zhao, Hang; Azar, Y.; Wang, K.; Wong, G.N.; Schulz, J.K.; Samimi, M. (January 1, 2013). "Millimeter Wave

Mobile Communications for 5G Cellular: It Will Work!". IEEE Access. 1: 335–349. doi:10.1109/ACCESS.2013.2260813. ISSN 2169-3536.

- Nordrum, Amy; Clark, Kristen (January 27, 2017). "Everything you need to know about 5G". IEEE Spectrum magazine. Institute of Electrical and Electronic Engineers. Archived from the original on January 20, 2019.
- Hoffman, Chris (January 7, 2019). "What is 5G, and how fast will it be?". How-To Geek website. How-To Geek LLC. Archived from the original on January 24, 2019.
- Segan, Sascha (December 14, 2018). "What is 5G?". PC Magazine online. Ziff-Davis. Archived from the original on January 23, 2019.
- Shatrughan Singh (March 16, 2018). "Eight Reasons Why 5G Is Better Than 4G". Altran. Archived from the original on May 25, 2019.
- G.Chalkiadakis, V. Robu, R.Kota, A. Rogers and N.R. Jennings. 2011. Cooperatives of distributed energy resources for efficient virtual power plants. In Proc. of 10th Intl. Conf. on Autonomous Agents and Multiagent Systems, May, 787–794.
- S.Chowdhury, S. Chowdhury and P. Crossley. 2009. Microgrids and Active Distribution Networks. Institution of Engineering and Technology (IET).
- E. Davidson, S. McArthur, C.Yuen and M.A. Larsson. 2008. Towards the delivery of smarter distribution networks through the application of multiagent systems technology. IEEE Power and Energy Society General Meeting, 1– 6.
- M.Deindl, C. Block, R. Vahidov and D.Neumann. 2008. Load shifting agents for automated demand side management in micro energy grids. In Proc. of 2nd IIEEE Intl. Conf. on Self-Adaptive and Self-Organizing Systems, 487–488.
- A. Dimeas and N.Hatziargyriou. 2007. Agent based control of virtual power plants. In Proc. of the Intl. Conf. on Intelligent Systems Applications to Power Systems, 1– 6.
- J. McDonald. 2008. Adaptive intelligent power systems: Active distribution networks. Energy Policy 36, 12, Foresight Sustainable Energy Management and the Built Environment Project, 4346–4351.
- S. Ramchurn, P. Vytelingum, A. Rogers and N.R. Jennings. 2011. Agent-based homeostatic control for green energy in the smart grid. ACM Transactions on Intelligent Systems and Technology, 2, May.
- S.D. Ramchurn, P. Vytelingum, A. Rogers and N.R. Jennings. 2011. Agent-based control for decentralized demand side management in the smart grid. In Proc. of the 10th Intl. Conf. on Autonomous Agents and Multiagent Systems. May, 5–12.
- P. Ribeiro, B. Johnson, M.Crow, A. Arsoy and Y. Liu. 2001. Energy storage systems for advanced power applications. In Proc. of IEEE 89, 12, 1744 – 1756.
- G. Strbac. 2008. Demand side management: Benefits and challenges. Energy Policy 36, 12, 4419–4426.

- **V. Sundramoorthy, G.Cooper, N. Linge and Q. Liu. 2011. Domesticating energy-monitoring systems: Challenges and design concerns. IEEE Pervasive Computing, 10, 20–27.**
- **P. Vovos, A. Kiprakis, A. Wallace, A. and G. Harrison. 2007. Centralized and distributed voltage control: Impact on distributed generation penetration. Power Systems, IEEE Transactions, 22, 1, 476– 483.**
- **P.Vytelingum, T.D.Voice, S.D., Ramchurn, A. Rogers and N.R.Jennings. 2010. Agent-based micro-storage management for the smart grid. In Proc. of 9th Intl. Conf. on Autonomous Agents and MultiAgent Systems, May, 39–46.**
- **EU SmartGrid Technology Platform. Vision and strategy for Europe's electricity networks of the future. Tech. Report, European Union, 2006.**
- **J. Froehlich, L. Findlater and J. Landay. 2010. The design of eco-feedback technology. In Proc. of 28th Intl. Conf. on Human Factors in Computing Systems. ACM, NY, 1999–2008.**
- **E.Rich and K. Night. 1991. Artificial intelligence. 2nd edition. Mcgraw-Hill, New York.**
- **H. Eriksson 1996. Expert system in knowledge servers. IEEE Expert.**
- **Y. Afek and S. Dolev. 2002. Local Stabilizer. Journal of Parallel and Distributed Computing, special issue on self-stabilizing distributed systems, Vol. 62, No. 5, pp. 745-765, May.**
- **E. Anceaume, X. Defago, X., M. Gradinariu and M.Roy. 2005. Towards a theory of self-organization. 9th International Conference on Principels of Distributed Systems, OPODIS, pp. 146-156.**
- **M.Chandy and L.Lamport. 1985. Distributed snapshots: determining global states of distributed systems. ACM Transactions on Computing Systems, 3(1):63-75.**
- **E.W. Dijkstra. 1974. Self-stabilizing systems in spite of distributed control. Communications of the ACM, 17(11):643-644.**
- **S. Dolev and T.Herman. 1995. Super Stabilizing Protocols for Dynamic Distributed Systems. Proc. of the 2nd Workshop on Self-Stabilizing Systems, May.**
- **S.Ghosh, A.Gupta, T.Herman and S. Pemmaraju. 1996. Fault-Containing Self-Stabilizing Algorithms. *PODC* 1996, pages 45–54.**
- **G. Varghese. 2000. Self-stabilization by counter flushing. SIAM Journal on Computing, 30(2):486-510.**
- **H. Zhang and A. Arora. 2002. GS3: Scalable Self-configuration and Self-healing in Wireless Networks. Symposium on Principles of Distributed Computing, pages 58-67.**
- **Clemente. 2009. The security vulnerabilities of smart grid. J. Energy Security, June.**
- **G. N. Ericsson. 2009. Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment and technology. IEEE Trans. Power Delivery, vol. 24, no. 3, pp. 1174–1181, July.**
- **P. McDaniel and S. McLaughlin. 2009. Security and privacy challenges in the smart grid. IEEE Security Privacy, vol. 7, no. 3, pp.75–77, May/June.**

- NIST. 2010. Guidelines for smart grid cyber security. The Smart Grid Interoperability Panel - Cyber Security Working Group, NISTIR 7628, Gaithersburg, MD, August.
- S. M. Amin. 2010. Securing the electricity grid. Bridge, vol. 40, no. 1, pp. 13–20, Spring.
- S. M. Amin. 2005. Energy infrastructure defense systems. Proc. IEEE, vol. 93, no. 5, pp. 861–875, May.
- S. M. Amin. 2004. Balancing market priorities with security issues: Interconnected system operations and control under the restructured electricity enterprise. IEEE Power Energy Mag., vol. 2, no. 4, pp. 30–38, Jul./Aug.
- J.Brocke, R. T. Watson, C. Dwyer, S. Elliot, and N. Melville. 2013. Green Information Systems: Directives for the IS Discipline. Communications of the Association for Information Systems 33 (1): 509--520.
- C. A. Santos, S. C. Romero, C. P. Molina, and M. Castro-Gil. 2012. Profitability Analysis of Grid-Connected Photovoltaic Facilities for Household Electricity Self-Sufficiency. Energy Policy 51 (December): 749–64.
- P. Cramton. 2017. Electricity Market Design. Oxford Review of Economic Policy 33 (4): 589–612.
- G. Christoph, H. Jacobsen, V. Razo, C. Doblander, J. Rivera, J. Ilg, C. Flath. 2014. Energy Informatics. Business & Information Systems Engineering 6 (1): 25–31.
- C.Loock, T. Staake and F. Thiesse. 2013. Motivating Energy-Efficient Behavior with Green IS: An Investigation of Goal Setting and the Role of Defaults. MIS Q. 37 (4): 1313–1332.
- N.P.Melville. 2010. Information Systems Innovation for Environmental Sustainability.MIS Quarterly, 34 (1): 1--21.
- M. Paschmann and S. Paulus. 2017. The Impact of Advanced Metering Infrastructure on Residential Electricity Consumption - Evidence from California. Working Paper WP 17/08. University of Cologne.
- P. Markus, W. Ketter, M. Saar-Tsechansky, and J. Collins. 2013. A Reinforcement Learning Approach to Autonomous Decision-Making in Smart Electricity Markets. Machine Learning, 92 (1): 5–39.
- S. Stefan, J. Recker, and J. Brocke. 2013. Sensemaking and Sustainable Practicing: Functional Affordances of Information Systems in Green Transformations. MIS Quarterly, 37 (4): 1275-A10.
- S. M. Godoy, R. Roche, E. Kyriakides, A. Miraoui, B. Blunier, K. McBee, S. Suryanarayanan, P. Nguyen, and P. Ribeiro. 2011. Smart-Grid Technologies and Progress in Europe and the USA. In Energy Conversion Congress and Exposition (ECCE), IEEE, 383–90.
- R.T. Watson, M. Boudreau, and A. J. Chen. 2010. Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. Management Information Systems Quarterly 34 (1): 4.
- https://www.power-technology.com/features/feature-upgrading-us-grid-smart-self-healing-reality accessed on 1.2.2019

- **A. Aggarwal, S.Kunta and P.K.Verma. 2010. A proposed communications infrastructure for the smart grid. Innovative Smart Grid Technologies, January,Gaithersburg, MD, pp.1–5.**
- **H. Khurana, M. Hadley, N. Lu and D.A. Frincke. 2010. Smart-grid security issues', Security Privacy. *IEEE*, Vol. 8,No. 1, pp.81 –85.**
- **Y. Liu, M.K.Reiter and P.Ning. 2009. False data injection attacks against state estimation in electric power grids. Proceedings of the 16th ACM Conference on Computer and Communications Security, *CCS '09*, ACM, NY, USA, pp.21–32.**
- **J.Lu, D. Xie and Q. Ai. 2009. Research on smart grid in China. Transmission Distribution Conference Exposition: Asia and Pacific, October, Seoul, Korea, pp.1–4.**
- **S.M. Amin and B.F. Wallenberg. 2005. Toward a smart grid: power delivery for the 21st century. Power and Energy Magazine, *IEEE*, Vol. 3, No. 5, pp.34–41.**
- **P. McDaniel and S. McLaughlin. 2009. Security and privacy challenges in the smart grid. Security Privacy, IEEE, Vol. 7, No. 3, pp.75 –77.**
- **Cen Nan, Faisal Khan, M. Tariq Iqbal. Real-time fault diagnosis using knowledge-based expert system. 2007.**
- **T.J.Parenty. 2003. Digital defense what you should know about protecting your company's assets. Harvard Business School Press.**
- **M.Hentea.2008. A perspective on security risk management of DCS control systems. Computers and Their Applications, 222-227.**
- **21 Steps to improve cyber security of SCDA networks. http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf accessed on 15.11.2012.**
- **W.R.Dunn. 2003. Designing safety critical computer systems. IEEE Computer, 36(11), 40-46.**
- **D.Geer. 2006. Security of critical control systems spark concern. IEEE Computer, 39(1), 21-23.**
- **S.S.Smith.2006.The SCADA Security challenge: The race is on. http://www.infosecwriters.com/text_resources/pdf/SSmith_DCS.pdf accessed on 15.11.2012.**
- **J.L.Hellerstein, Y. Diao, S.Parekh and D.M.Tilbury.2005. Control engineering for computing systems. IEEE Control Systems Magazine. 25(6), 56-68.**
- **M.Gertz and S.Jajodia. 2008. Handbook of database security applications and trends.**
- **S.Kumar.1995. Classification and detection of computer intrusions. Thesis, Purdue University.**
- **J.Douceur. 2002. The sybil attack. Proceedings of Workshop on P2P systems (IPTPS).**
- **S.Zhu, S.Xu and S.Jajodia. 2003. LEAP: Efficient security mechanisms for large scale distributed sensor networks. Proceedings of 10th ACM Conference on Computer and Communication Security, 62-72.**

- **W.Du, D.Jeng, Y.Han and P. Varshney. 2003. A pairwise key predistribution schemes for wireless sensor networks. Proceedings of 10th ACM Conference on computer and communication security (CCS'03).42-51.**
- **D.Jeng, R.Han and S.Mishra. 2004. Intrusion tolerance strategies in wireless sensor networks. Proceedings of IEEE International conference on dependable systems and networks.**
- **H.Chan, A. Perrig and D.Song.2003. Random key predistribution schemes for sensor networks. Proceedings of IEEE security and privacy symposium.**
- **D.Choi, S.Lee, D.Won and S.Kim.2010. Efficient secure group communication for SCADA. IEEE Transactions on power delivery, volume 25, no. 2.**
- **R.D. Colin, C. Boyd, J.Manuel and J.Nieto, 2006. KMA - A key management architecture for SCADA system. Proceedings of 4th Australian Information Security Workshop, volume 54, 138-197.**
- **J. Pollet. 2002. Developing a solid DCS security strategy. SICON'02, Texas, USA.**
- **A.R.Metke and R.L. Ekl. 2010. Plant security technology, Motorola Inc., USA, IEEE.**
- **M.Naedele.2007. Addressing IT security for critical control systems. ABB Corporate Research. Proceedings of 40th HICSS.**
- **T.Seki, T.Takehino, T.Tanaka, H.Watanabe and T.Seki. 2000. Network integrated supervisory control for power systems based on distributed objects. SAC'00, Italy.**
- **A.Seshadri, A.Perrig, L.van Doorn and P.Khosla.2004. SWATT: Software based attestation for embedded devices. Proceedings of IEEE Symposium on Security and Privacy, Oakland, California.**
- **www.theresilienterprise.com accessed on 15.11.2012**
- **Berard, B., Bidoit,M., Finkel,A., Laroussinite, F., Petit, A., Petrucci, L., Schnoebelen, Ph., Mckenzie,P. 2001. Systems and software verification. Springer.**
- **Y.Liu, P.Ning and M.K.Reiter. 2009. False data injection attacks against state estimation in electric power grid. CCS'09, Chicago, Illinois, USA.**
- **A.Studer and A.Perrig.2008. The Coremelt attack.**
- **J.M.Colbert and A.Kott (Editors). 2016. Cyber security of SCADA and other industrial control systems. Springer, Switzerland.**
- **S. Forrest et al. 1994. Self-Nonself Discrimination in a Computer. In Proceedings of IEEE; Computer Society Symposium on Research in Security and Privacy, pp. 202–212.**
- **J.Kim et al. 2007: Immune system approaches to intrusion detection - a review. Natural Computing 6(4), 413–466.**
- **W.Lee, J.S.Salvatore and K.W.Moke 2000. Adaptive intrusion detection: a data mining approach. Kluwer Academic Publishers, Netherlands.**
- **P.Matzinger P. 1994. Tolerance Danger and the Extended Family, Annual reviews of Immunology 12, pp 991-1045.**
- **P.Matzinger 2002. The Danger Model: A Renewed Sense of Self, Science 296: 301-305.**

- **U.Aickelin and S.Cayzer. 2002. The Danger Theory and Its Application to AIS, 1st International Conference on AIS, pp 141-148.**
- **A.K.Jain. 2007. Biometric recognition. Nature, 449:38-40.**
- **S.Prabhakar, S.Pankanti and A.K.Jain.2003. Biometric recognition: security and privacy concerns. IEEE security and privacy magazine. 1(2):33-42, March - April.**
- **R.Bottle, J.Konnell, S.Pankanti, N.Ratha and A.Senior. 2003. Guide to Biometrics. Springer.**
- **M.Shema. edited by A.Ely. 2010. Seven deadliest web application attacks. Elsevier.**
- **S.Nikoletseas and J.D.P.Rolim.2010. Theoretical aspects of distributed computing in sensor networks. Springer.**
- **C.K.Wong, M.Gouda & S.S.Lam. 2000. Secure group communications using key graph, IEEE/ACM Transactions on Networking, 18(1).**
- **S. Chakraborty. 2007. A study of several privacy preserving multi-party negotiation problems with applications to supply chain management. Thesis guided by Prof. A.K.Pal. Indian Institute of Management Calcutta, India.**
- **A.K.Pal, D.Nath and S. Chakraborty. 2010. A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor, WASET.**
- **H. Sundmaeker, P. Guillemin, P. Friess, P. and S., Woelfflé (eds.), 2010. Vision and Challenges for Realising the Internet of Things. CERP-IoT, European Commission.**
- **K. Pretz 2013. The Next Evolution of the Internet. The Institute, IEEE (January 7, 2013), http://theinstitute.ieee.org/technology-focus/technologytopic/**
- **the-next-evolution-of-the-internet**
- **P.C. Evans, M. Annunziata 2012. Industrial Internet: Pushing the boundaries of minds and machines. GE report, March. http://www.ge.com/docs/sessions/Industrial_Internet.pdf**
- **H. LeHong and J. Fenn. 2012. Key Trends to Watch in Gartner 2012 Emerging Technologies Hype Cycle.**
- **PM Frank, SX Ding, and T Marcu. Model-based fault diagnosis in technical processes. Transactions of the Institute of Measurement and Control, 22(1):57–101, 2000.**
- **D.M. Himmelblau. Fault detection and diagnosis in chemical and petrochemical processes. Chemical engineering monographs. Elsevier Scientific Pub. Co., 1978.**
- **R. Isermann. Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance. Springer, 2006.**
- **Chen Ming, Zhou Runqing, Zhang Rui, and Zhu Xianzhong. Application of artificial neural network to failure diagnosis on process industry equipments. In Natural Computation (ICNC), 2010 Sixth International Conference on, volume 3, pages 1190–1193. IEEE, 2010.**
- **Venkat Venkatasubramanian, Raghunathan Rengaswamy and Surya N Kavuri. A review of process fault detection and diagnosis: Part ii: Qualitative**

models and search strategies. Computers & Chemical Engineering, 27(3):313–326, 2003.

- Venkat Venkatasubramanian, Raghunathan Rengaswamy, Surya N Kavuri, and Kewen Yin. A review of process fault detection and diagnosis: Part iii: Process history based methods. Computers & chemical engineering, 27(3):327–346,2003.
- Venkat Venkatasubramanian, Raghunathan Rengaswamy, Kewen Yin, and Surya N Kavuri. A review of process fault detection and diagnosis: Part i: Quantitative model-based methods. Computers & chemical engineering, 27(3):293–311,
- Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. In ICS 2010, 2010.
- Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. arXiv preprint arXiv:1704.04487, 2017.
- Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive, 2018.
- Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications. In CRYPTO, 2010.
- Sergei Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates andnoisy ancillas. Physical Review A, (022316), 2005.
- Michael Ben-Or, Claude Cr´epeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In FOCS'06, 2006.
- Anne Broadbent and EvelynWainewright. Efficient simulation for quantum message authentication. In ICITS 2016, 2016.
- Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In CCS '17, 2017.
- Ronald Cramer, Ivan Damg°ard, and Jesper Buus Nielsen. Secure Multiparty Computation and Secret Sharing. Cambridge University Press, 2015.
- Claude Cr´epeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. In STOC, 2002.
- Fr´ed´eric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In CRYPTO, 2010.
- Fr´ed´eric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In CRYPTO. 2012.
- Elham Kashefi, Luka Music, and PetrosWallden. The quantum cut-and-choose technique and quantum two-party computation. arXiv preprint arXiv:1703.03754, 2017.
- Elham Kashefi and Anna Pappa. Multiparty delegated quantum computing. Cryptography, 1(2), 2017.

- **Dominique Unruh. Universally composable quantum multi-party computation. In EUROCRYPT, 2010.**
- **Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In FOCS ’82, 1982.**
- **I. L. Chuang and Y. Yamamoto. Simple quantum computer. Phys. Rev. A, 52:3489–3496, 1995. arXive e-print quant-ph/9505011.**
- **Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton, Cryptographic primitives based on hard learning problems, Advances in Cryptology, CRYPTO, Lecture Notes in Computer Science, vol. 773, Springer, 1993, pp. 278–291.**
- **Burton H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM 13 (1970), 422–426.**
- **Andrei Broder and Michael Mitzenmacher, Network applications of Bloom filters: A survey, Internet Mathematics, 2002, pp. 636–646.**
- **Oded Goldreich, The foundations of cryptography - volume 1, basic techniques, Cambridge University Press, 2001.**
- **Moni Naor and Eylon Yogev, Sliding Bloom filters, Algorithms and Computation - 24th International Symposium, ISAAC, vol. 8283, Springer, 2013, pp. 513–523.**
- **Rasmus Pagh, Cuckoo hashing, Encyclopedia of Algorithms, Springer, 2008.**
- **Rasmus Pagh and Flemming Friche Rodler, Cuckoo hashing, Journal of Algorithms 51 (2004),no. 2, 122–144.**
- **Moni Naor and Eylon Yogev. Bloom Filters in Adversarial Environments. arXiv:1412.8356v2 [cs.CR] 15 Feb 2015**
- **B. Fan, D. Andersen, M. Kaminsky and M. Mitzenmacher \Cuckoo Filter: Practically Better Than Bloom" in Proceedings of CoNext 2014.**
- **B.E.Boser, I.M.Guyon, and V.N.Vapnik, A training algorithm for optimal margin classifiers. In D.Haussler, Editor, Proceedings of the 5th Annual ACM Workshop On Computational Learning Theory, pages 144-152, ACM Press, 1992.**
- **N. Cristianini And J.S.Taylor, An Introduction to Support Vector Machines and other kernel based learning methods, Cambridge University Press, 2000.**
- **V.N.Vapnik, Statistical Learning Theory, John Wiley & Sons Inc., 1998.**

Quiz

- **Explore the scope of digital technologies for the future. Justify the same as technologies for humanity.**
- **Identify dominant design schema of various emerging digital technologies.**
- **What are the basic elements of the system architecture associated with various digital technologies?**
- **What do you mean by security of digital technologies? How can You verify the security intelligence? Design adaptive security algorithms and dynamic data protection mechanisms.**
- **What are the strategic moves of innovation, adoption and diffusion of digital technologies? What is the outcome of technology life-cycle analysis?**
- **How can you manage resources for digital technology innovation projects?**

- **What should be the talent management strategy? What are the skills, leadership style and support demanded by digital technology innovation?**
- **How can You manage digital technology innovation project efficiently? What should be the shared vision, common goals and communication protocols? How can you ensure a perfect fit among '7-S' elements?**
- **Compare the strength, weakness, opportunities and threats of 4G,5G,6G and 7G mobile communication technologies.**
- **Discuss the strength and weakness of various models of cloud computing and also exercise SWOT analysis of cloud computing and cloud streaming technologies.**
- **Define solar computing. What is the scope of solar computing innovation?**
- **What is the dominant design of solar computing innovation?**
- **What are the basic elements of the system architecture associated with solar computing innovation? How to represent the structure correctly?**
- **What do you mean by technology security for solar computing ? How to verify the security intelligence? What is the role of adaptive security and dynamic data protection in solar computing? Design an adaptive security architecture. Develop a self-healing mechanism.**
- **What are the strategic moves of technology innovation, adoption and diffusion of solar computing? What is the outcome of technology life-cycle analysis?**
- **How to manage resources in solar computing innovation project? What should be the talent management strategy?**
- **What are the skills, leadership style and support demanded by the technological innovation in solar computing ?**
- **How to manage technology innovation project in solar computing efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements?**
- **Case study : Please study following case study and outline a smart grid to tackle disruption of energy and utility service and improve resiliency.**

From : A chakraborty (achakraborty2020@hootmail.com)
To: smu.hfw.wb@cmail.com
Cc: connect@mygov.nic.im ; PTDlimited@wb.gov.im; powersecy@wb.gov.im
Sun 4/24/2019 3:34 PM
Subject : Bioterrorism, Epidemic, Cyclone....
Respected Sir / Madam,
I would like to share real-life experience and observations during locked down West Bungul for your thoughts. I would also like to bring to your attention for necessary BPR initiatives, fundamental rethinking and radical redesign of power generation and distribution system in terms of scope, system, structure, security, strategy, staff-resources and skill-style-support.
High tariff rate : As-is tariff rate is high in our state as compared to power generation and distribution companies of other states of the country. The adoption

of solar microgrid as clean energy may reduce the cost of coal based thermal power in future. There are threats of global warming, extreme weather conditions and issues of environmental pollution. Standalone rooftop solar panel system is useful as source of back up energy supply during natural disaster. The public may not become violent, unrest or impatient due to disruption in supply of energy and utility (e.g. water, mobile) as inevitable consequences of natural disaster

The consumers are confused about the logic of computation of electric billing system. For example, the meter reading was not taken in March'2020 and April'2020 by your staff. The bill of March'2020 considered the units consumption of March'2019 but the same logic was not followed in April'2020. The consumers are facing problems to pay through offline channels. It is basically an issue of fairness, correctness, rationality, transparency and trust in financial accounting. (Ref. : bills of March'2020 and April'2020). Donation of power for religious festivals may not be a lame excuse; it may be a classic case of money laundering in India Today.

The power tariff is high but there are instances of disruption in power supply and QoS. For example, there was severe voltage regulation problems for one hour, frequent on and off of power supply and major cable fault between 7-00 and 19-30 on 17.5.2020 in my locality. There was also power cut on 18.5.2020 and 20.5.2020, 3 hours during cyclone. But, the critical issue is that power was not shut down even half an hour later the start of the cyclone. It took twelve hours on 17.5.2020 to rectify the power system fault. There might be severe negative impact on the performance of domestic electrical and electronic devices and also surge in meter reading due to such abnormal electrical conditions i.e. switching surges ON OFF ON OFF ON OFF.. As an Electrical Engineer, I am shocked and surprised at the responsible role and effectiveness of supervisory control and data acquisition (SCADA) control system of Power Distribution company. Is it a classic case of failure of control system? Power cut may happen due to various problems: system failure, natural disaster, demand-supply gap, power play and politics and also industrial unrest. Such type of power cut in summer may cause fever, cold, cough and respiratory problems and the epidemic and pandemic subsequently.

The staff of electric power distribution companies often dig roads for electrical repair and maintenance works but the roads are often not repaired in time resulting dens and path holes here and there on the busy road. Such type of casual work culture imposes threats of safety of common people and the drivers particular during rainy season and in the darkness of night.

The Civic Volunteers Force and the security staff are expected to be properly trained and educated on various issues : attitude, behavior, public relationship management, creating unnecessary panic riding bikes with horn at high speed, random lathi charge on innocent street sellers and common people in spite of giving proper explanation of emergency situation modestly.

Use of mask for long duration creates a suffocated congested unhealthy environment to each user due to inhaling of CO and CO_2, the byproducts of own respiration. Corporate healthcare communication should look into this issue carefully, cautiously and practically. The cotton and textile industries should be promoted rationally, not causing healthcare ailments!

Sequential workflows and social distancing are creating long waiting time in the queue of the public in hot sunshine before banks, post offices, grocery shops and medicine shops. Such process flow may cause indirectly fever, cold, cough and respiratory problem of the public particularly senior citizen.

Door to door service of food and beverages may break the safety and privacy of common healthy public. It may be taken as the reference of the death of the film director Kiddu who used to take food through door-to-door delivery service. It may be recalled the murder of an honest journalist by the malicious adversaries in the film 'Sridev' through door-to-door service of poisonous milk.

Request for your attention and intervention to look into the aforesaid issues on urgent basis for exploring good solutions in future. I have shared my learning, observation and perception which needs correct validation.

Regards.

A Chakraborty

BEE(KU), Fellow (IIMW), Consumer no. :56200061009, Phone : 8840477441, West Bungal -722206, "

- **Define ISI analytics. What is the scope of ISI analytics from the perspectives of IIoT? What are the differences between IoT and IIoT? What are the strength and weaknesses of IIoT?**
- **What is the dominant design of ISI analytics?**
- **What are the basic elements of the system architecture associated with ISI analytics? How to represent the structure correctly for SCADA and ICS?**
- **What do you mean by technology security for IIoT enabled SCADA and ICS? How to verify the security intelligence? What is the role of adaptive security and dynamic data protection in IIoT? Design an adaptive security architecture. Develop a DDP algorithm.**
- **What are the strategic moves of technology innovation, adoption and diffusion of ISI analytics? What is the outcome of technology life-cycle analysis?**
- **How to manage resources in SCADA / ICS innovation project? What should be the talent management strategy?**
- **What are the skills, leadership style and support demanded by the technological innovation of ISI analytics?**
- **How to manage technology innovation project in ISI analytics efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements?**
- **Define secure multi-party quantum computing. What is the scope of SMQC?**
- **What is the dominant design of quantum computers?**
- **What are the basic elements of the system architecture associated with SMQC?**
- **How to represent the structure of SMQC in terms of quantum bits, gates and circuits?**
- **What do you mean by security of quantum computing ? How to verify the security intelligence? What is the role of adaptive security and dynamic data protection in SMQC? Design an adaptive security architecture.**
- **What are the strategic moves of technology innovation, adoption and diffusion of SMQC? What is the outcome of technology life-cycle analysis?**

- **How to manage resources in SMQC technology innovation? What should be the talent management strategy? What are the skills, leadership style and support demanded by the technological innovation of SMQC ?**
- **How can you ensure a perfect fit among '7-S' elements?**
- **Define a secure adaptive filter and state its features and functions. What is the scope of secure adaptive filter? What are the similarities and differences between Bloom and Adaptive Cuckoo filter? What are the strength and weaknesses of these filters?**
- **What is the dominant design of a secure adaptive filter? Analyze the complexity of this technology based on aforesaid algorithmic mechanism? Construct private support vector algorithm for packet classification by seure adaptive filter.**
- **What are the basic elements of the system architecture associated with secure adaptive filter? Compare various types of adaptive filters.**
- **What do you mean by security of adaptive filter technology? How to verify the security intelligence of adaptive filter? Discuss various issues of private classification by secure adaptive filter?**
- **What are the strategic moves of technology innovation, adoption and diffusion of secure adaptive filter? What is the outcome of technology life-cycle analysis?**
- **How to manage resources in innovation of secure adaptive filter? What should be the talent management strategy?**
- **What are the skills, leadership style and support demanded by the technological innovation of ISI analytics?**
- **How to manage technology innovation project of secure adaptive filters efficiently?**
- **What should be the shared vision, common goals and communication protocols?**
- **How can you ensure a perfect fit among '7-S' elements for the innovation, adoption and diffusion of adaptive filter technology?**

Sumit Chakraborty is one of the authors of this book. He had done his graduation in Electrical Engineering from Jadavpur University and attended Fellow programme at IIM Calcutta. His major area was Management Information Systems (MIS) and minor area was Strategic Management. He worked in in power project management, power transmission and distribution and global supply chain management and ERP for a manufacturing plant and in business consulting such as process mapping and requirements management. He has also made modest efforts to carry out research in MIS, Information Security and business analytics. He has taught courses at various management institutes in India. Suryashis Chakraborty is the co-author. He has done his graduation in Business Administration. Kusumita Chakraborty, another author of this book did her graduation (Honours), post graduation and doctoral thesis on education from CU. The authors have interest in business analytics, data science and technology for humanity.